Implementing Efficient Monitoring And Data Dynamics For Data Storage Security in Cloud Computing

[1]Pavithra S.,
[1]Assistant Professor,
Vel Tech Multitech Dr.RR & Dr. SR Engg College
E-mail: pavi_eye@yahoo.co.in

[2]Badi Alekhya.,
[2] M.E- Student,
Vel Tech Multitech Dr.RR & Dr.SR Engg College
E-mail: alekhyareddy1@gmail.com

***Abstract*—Cloud Computing is an internet based computing that enables sharing of resources. This project supports an external auditor to audit user's outsourced data in the cloud with out learning knowledge on the data content. This Project is the first to support scalable and efficient public auditing in the Cloud Computing by using AES (Advanced Encryption Standard) and MD5 (Message Digest) Algorithms. In particular, it achieves batch auditing using scheduling policies where multiple delegated auditing tasks from different users can be performed simultaneously by the Third Party Auditor. Achieving the Data Dynamics is also important.**

Keywords: **Data Dynamics, Cloud Computing, Advanced Encryption Standard, Message Digest.**

I. INTRODUCTION

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high quality services from data and software that reside solely on remote data centers.

Cloud computing technology has been a new buzzword in the IT industry and expecting a new horizon for coming world. It is a style of computing which is having dynamically scalable virtualized resources provided as a service over the Internet. It reduces the time required to procure heavy resources and boot new server instances in minutes, allowing one to quickly scale capacity, both up and down, as ones requirement changes. Nevertheless the technology is hot in the market and is ready to cater to the small and medium business segment. As per one of the estimates from Gartner, by year 2012, 20% of enterprise market e-mail seats will be delivered via Cloud. As per another estimate from Gartner, Software as a Service is forecast to have a compound annual growth rate of 17% through 2011 for CRM, ERP and SCM markets in SMB segment. While the enterprises are exploring the possibilities of adopting this technology, it is imperative for these enterprises to critically evaluate the feasibility of this technology for their specific businesses.

A. The Typical Characteristic of this Technology:

Cloud computing customers do not generally own the physical infrastructure serving as host to the software platform in question. Instead, they avoid capital expenditure by renting usage from a third-party provider. The entire onus lies on the service provider who owns the huge scalable and variable host of infrastructure, software and bundle of other services. Cloud computing consumers consume resources as a service and pay only for resources that they use. Many cloud-computing offerings employ the utility computing model, which is analogous to how traditional utility services (such as electricity) are consumed, while others bill on a subscription basis. Sharing "perishable and intangible" computing power among multiple tenants can improve utilization rates, as servers are not unnecessarily left idle (which can reduce costs significantly while increasing the speed of application development).

Cloud computing is emerging at the convergence of three major trends — service orientation, virtualization and standardization of computing through the Internet. Cloud computing enables users and developers to utilize services without knowledge of, expertise with, nor control over the technology infrastructure that supports them. The concept generally incorporates combinations of the following:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

B. Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired

applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

C. Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

D. Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

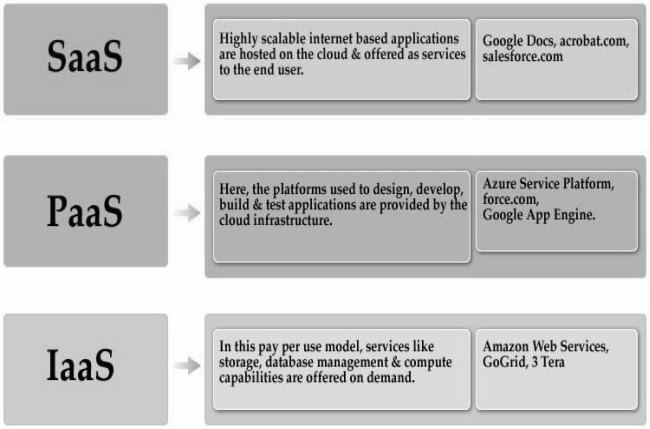

Figure 1. Service Models

E. Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.

The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.
Forrester defines cloud computing as:

A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption.

II. PROBLEM DEFINITION

One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files.

III. PROBLEM OBJECTIVE

In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and retrievability of data, etc. Consider the role of the verifier in the model, all the schemes presented before fall into two categories: private auditability and public auditability. Although schemes with private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their

computation resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public auditability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. Moreover, for efficiency consideration, the outsourced data themselves should not be required by the verifier for the verification purpose.

IV. DEPLOYMENT MODELS

A. Private cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

B. Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

C. *Public cloud*

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

D. *Community cloud*

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

E. *Hybrid cloud*

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

F. *Pros and Cons of Cloud Computing*

Cloud Computing focuses on providing access for users to services, applications or storage without actually having to reveal any of the underlying technology and science behind how the elements are made to work. There are numerous pros and cons for the use of Cloud Computing, with different pros and cons applying to different applications and usages. Cloud computing is not for everyone, so understanding the pros and cons is important in determining how it can impact your business.

G. *Scale and Cost*

The cost associated with cloud computing is said to be one of its greatest pros because costs are greatly reduced. Capital expenditure, also, is converted into operational expenditure. Another great benefit of cloud computing is the scalability, as on demand provisioning for resources makes it possible for cloud computing to offer greater scalability for many business types that use web services as their system interface.

H. *Encapsulated Change Management*

Encapsulated change management offered by cloud competing achieves a number of different business goals and business objectives, including improvements in customer service and in service delivery. Encapsulated change management may also lower working capital requirements while aiding in the management of resources and fixed assets.

I. *Next Generation Architectures*

Social networking and social media technologies are becoming increasingly important as a manner in which customers can find the information that they need. Cloud computing is utilizing these next generation technologies and architectures in order to allow companies to benefit from the web.

J. *Choice and Agility*

Cloud computing provides a great amount of choice for the businesses utilizing it, and the customers that rely on it to find the information that they need. Cloud computing is an agile technology that offers benefits to the businesses that decided to utilize its principles.

K. *Security*

While in some situations security is improved in cloud computing over other similar technologies, this is not always the case. There are concerns regarding loss of control over data that is sensitive, as well as concern over the lack of security over stored kernels, while security is being improved overtime.

L. Lock-in

Many of the currently emerging platforms for cloud computing are proprietary in nature, and what this means is that interoperability and portability are both going to be issues for many businesses. I believe the next big talk will be not about cloud computing but about how to connect different clouds without any hassle or they are already connected for the customers, and the customer will have a choice to switch between any cloud computing vendor.

M. Lack of Control

When the cloud computing system goes down, business managers can find themselves feeling completely helpless because they suddenly have no visibility of the infrastructure. Cloud computing can provide somewhat of a feeling of lack of control, where business owners find themselves having to rely on someone much higher up to find and rectify the issue.

N. Reliability

While cloud computing may be suitable for disaster recovery and business continuity, some major cloud computing services have experienced outages, and sometimes little can be done when businesses are affected.

Good thing is almost close to start trusting the reliability of this cloud ecosystem.

O. Cloud Storage

- Several large Web companies (such as Amazon and Google) are now exploiting the fact that they have data storage capacity which can be hired out to others.
- This approach, known as 'cloud storage' allows data stored remotely to be temporarily cached on desktop computers, mobile phones or other Internet-linked devices.
- Amazon's Elastic Compute Cloud (EC^2) and Simple Storage Solution (S3) are well known examples.

P. Uses of cloud

- It enables services to be used without any understanding of their infrastructure.
- Cloud computing works using economies of scale. It lowers the outlay expense for start up companies; as they would no longer need to buy their own software or servers. Cost would be by on-demand pricing. Vendors and Service providers claim costs by establishing an ongoing revenue stream.
- Data and services are stored remotely but accessible from 'anywhere'.

V. ARCHITECTURAL REPRESENTATION

The client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. Finally, find that file is sent to the client. If the server finds the intruder means, it will set the alternative Path to that intruder.

Cloud computing components are classified as 1) Cloud User (CU), 2) Cloud Service provider (CSP) and 3) Cloud server (*CS).*

Three different network can be identified as follows: Client: an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations;. Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data;. Third Party Auditor: an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As clients no longer possess their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies.

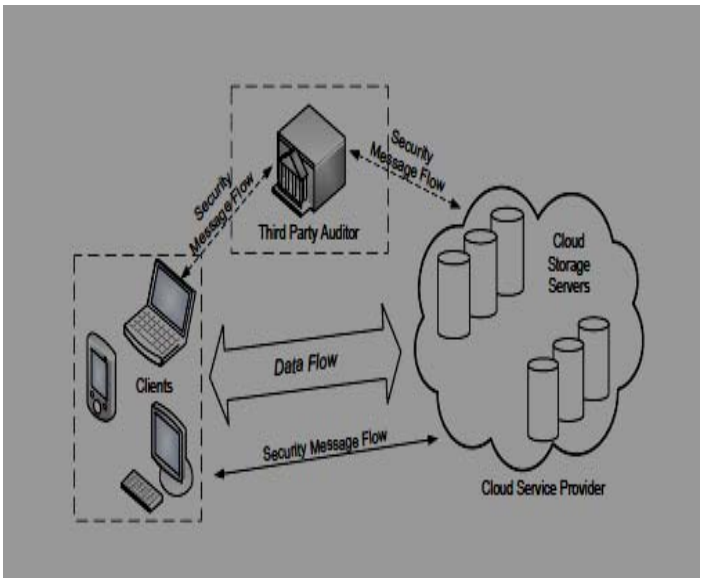

Figure 2. Representative network architecture for cloud data storage

In case that client do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA. In this paper, it only considers verification schemes with public auditability: any TPA in possession of the public key can act as a verifier. That TPA is unbiased while the server is untrusted. For application purposes, the clients may interact with the cloud servers via CSP to access or retrieve their pre stored data. More importantly, in practical scenarios, the client may frequently perform block-level operations on the data files. The most general forms of these operations consider in this paper are modification, insertion, and deletion. Note that it don't address the issue of data privacy in this paper, as of data privacy in Cloud Computing is orthogonal to the problem.

CONCLUSION

The 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. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. It utilize the symmetric key approach AES(Advanced Encryption Standard)and

MD5(Message Digest)efficient public auditing in the Cloud .It uses Scheduling policies for achieving Multiple Batch Auditing for multiple user Environment.

REFERENCES

[1] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica,M. Zaharia, "Above the clouds: A berkeley view of cloudcomputing," University of California, Berkeley, Tech. Rep,2009.

[2] Cong Wang, Qian Wang, Kui Ren,Wenjing Lou(2009),"Ensuring Data Storage Security in Cloud Computing".

[3] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou (2010),"Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing".

[4] A. L. Ferrara, M. Greeny, S. Hohen berger, M. Pedersen(2009), "Practical short signature batch verification", in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, pp. 309–324.

[5] H. Shacham, B. Waters (Dec 2008), "Compact proofs of retrievability ", in Proc. of Asia crypt 2008, vol. 5350,pp. 90–107

[6] M.A. Shah, R.Swaminathan, M. Baker (2008), "Privacy preserving audit and extraction of digital contents", Cryptology ePrint Archive.

[7] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou (2009), "Enabling public verifiability and data dynamics for storage security in cloud computing", in Proc. of ESORICS'09, Saint Malo.

[8] Wang, K. Ren, W. Lou (2010), "Achieving secure, scalable ,and fine-grained access control in cloud computing", Proc.of IEEE INFOCOM'10, San Diego, CA, USA.

[9] [Online] Available: Amazon.com, "Amazon s3 availability event: (2008)," Online at http://status.aws.amazon.com/ s3- 20080720.html.

[10] Cloud Security Alliance, (2009) "Security guidance for critical areas of focus in cloud computing," 9, [Online] Available http://www.cloudsecurityalliance.org

[11] P. Mell, T. Grance , (2009) "Draftnist working definition of cloud computing," Referenced on June. 3rd, 2009 on linear http: // csrc.nist.gov/groups/SNS/cloud-computing/index.html.

[12] Craig Gentry, Dan Boneh, (2004) "Aggregate and verifiablyencrypted signatures from bilinear maps".