IPHV2I10018X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SLA BASED DATA INTEGRITY IN CLOUD SERVERS

[1]PISKA VIJETHA, [2] UPPALAPATI SAROJA, [3]B.VEERA PRATHAP

1. M.Tech-(SE) Pursuing, 2. M.Tech-(SE) Pursuing ,
3. HOD, Dept of CSE, MOTHER THERESSA COLLEGE OF ENGINEERING & TECHNOLOGY

ABSTRACT

Cloud computing is the new era of service marketing, recently the cost of services are increased by cloud servers. The cost of service maintenance is hike due to the high costs of data storage devices and or individual users to frequently update their hardware. Instead of enterprise level or individual maintenance of data are out sourced to cloud servers. Cloud storage moves the user's data to large data centers, which are remotely located, on which user does not have any control. By this features leads to so many security issues are considered and cost reduction methods are focused in this article.

Keywords: cloud servers, data integrity, services, SLA.

INTRODUCTION

What is Cloud Computing

Cloud computing is a service that helps you to perform the tasks over the Internet. The users can access resources as they need them.

The term " Cloud" refers the internet. Cloud computing consists of hardware and software available on the internet managed by third party services.The authorized user can reach the cloud for resources when they need it. The users can manage their data in cloud by storing it in various devices.It is one of the best way to run business. The data stored in the cloud are accessed by the authenticated users via passwords or tokens the users just 'Plug in' and access the resources. The company or the individuals are paying for not using the system but now they can pay only for the computing power and services they use. The online storage is safe and secured. You just need the personal computer with internet connection. You need to have access to the cloud services to make use of it. Put whatever you want inside the cloud or make use of servers, software's, etc., you need. Disconnect it once you have done and release it back to the cloud. Pay

for the server utilized, processing power used and bandwidth consumed.

Best Example for Cloud Computing

Electricity Bill

Turn on your lights and meter starts running. Once it is switched off, meter stops.

You will pay only for the power utilized.

The same concept applies in the Cloud Computing. " Pay for what you use"

Types of cloud

Public Cloud- The cloud is available to all the users to utilize the resources. E.g., Google AppEngine, etc. Private Cloud- The cloud will be available with in the organization, not visible to external users.

Hybrid Cloud- Combination of both Public (External) and Private(Internal) Cloud.

Levels of Cloud Computing

There are three levels of Cloud Computing and are as follows:

Applications in the Cloud

Platforms in the Cloud

Infrastructure in the Cloud

Applications in the Cloud

The applications hosted in the Internet are offered as a service The user can sign up for and use without any concern about the computing power and storage capacity

Multi- users can access applications at the same time No installation or Upgrades required E.g., Gmail, Yahoo Mail, Wikipedia.etc.,

Platforms in the Cloud

The platforms are offered as a service in Cloud Develop your own code through web browser and upload it into the cloud to deploy it.

The code will magically run somewhere in the cloud without any server, Operating System or even without databases If the code grows, the cloud automatically scales up and down, to match the demand. No infrastructure cost and can deploy the application instantly.

Infrastructure in the Cloud

The Hardware and Data centers are offered as a services in the Cloud. With Cloud Computing, No need to spend time and costs to set up the Infrastructure. You can own your own Virtual data center for storage by keeping costs to a minimum.

No physical location of the resources, no maintenance cost and no operating cost.

Advantages

It is highly reliable, stable and easy to use

It reduces the capital costs and operation costs for the company.

It increases the Productivity and improves Compliance.

Finally, it reduces the overall cost and helps you to keep the upfront costs to a minimum.

Existing System

As data generation is far outpacing data storage it proves costly for small firms to frequently update their hardware whenever additional data is created. Also maintaining the storages can be a difficult task. It transmitting the file across the network to the client can consume heavy bandwidths. The problem is further complicated by the fact that the owner of the data may be a small device, like a PDA (personal digital assist) or a mobile phone, which have limited CPU power, battery power and communication bandwidth.

Disadvantages

- The main drawback of this scheme is the high resource costs it requires for the implementation.
- Also computing hash value for even a moderately large data files can be computationally burdensome for some clients (PDAs, mobile phones, etc).
- Data encryption is large so the disadvantage is small users with limited computational power (PDAs, mobile phones etc.).

Proposed System

One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. In this paper we provide a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA). It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

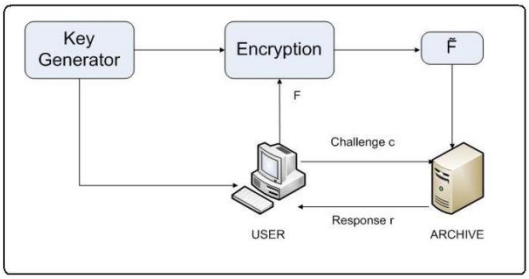
Advantages

Apart from reduction in storage costs data outsourcing to the cloud also helps in reducing the maintenance.

IPHV2I10018X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Avoiding local storage of data. By reducing the costs of storage, maintenance and personnel. It reduces the chance of losing data by hardware failures. Not cheating the owner.

Architecture:



Meta-Data Generation:

Let the verifier V wishes to the store the file F with the archive. Let this file F consist of n file blocks. We initially preprocess the file and create metadata to be appended to the file. Let each of the n data blocks have m bits in them. A typical data file F which the client wishes to store in the cloud.

Each of the Meta data from the data blocks mi is encrypted by using a suitable algorithm to give a new modified Meta data Mi. Without loss of generality we show this process by using a simple XOR operation. The encryption method can be improvised to provide still stronger protection for verifier's data. All the Meta data bit blocks that are generated using the above procedure are to be concatenated together. This concatenated Meta data should be appended to the file F before storing it at the cloud server. The file F along with the appended Meta data e F is archived with the cloud.

Cloud Storage:

Data outsourcing to cloud storage servers is raising trend among many firms and users owing to its economic advantages. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which is supposed to - presumably for a fee - faithfully store the data with it and provide it back to the owner whenever required.

Simply Archives:

This problem tries to obtain and verify a proof that the data that is stored by a user at remote data storage in the cloud (called cloud storage archives or simply archives) is not modified by the archive and thereby the integrity of the data is assured. Cloud archive is not cheating the owner, if cheating, in this context, means that the storage archive might delete some of the data or may modify some of the data. While developing proofs for data possession at untrusted cloud storage servers we are often limited by the

IPHV2I10018X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

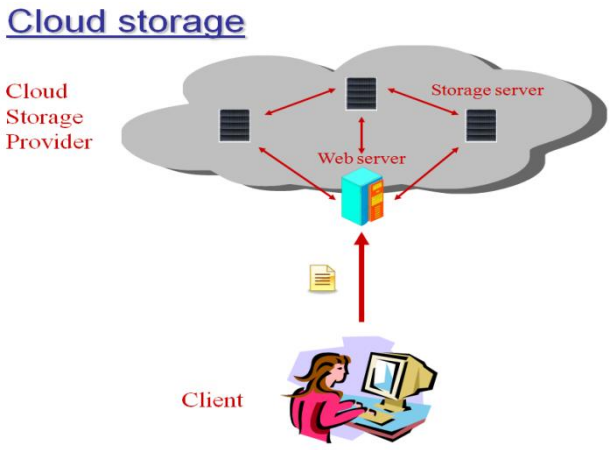
resources at the cloud server as well as at the client.

Sentinels:

In this scheme, unlike in the key-hash approach scheme, only a single key can be used irrespective of the size of the file or the number of files whose retrievability it wants to verify. Also the archive needs to access only a small portion of the file F unlike in the key-has scheme which required the archive to process the entire file F for each protocol verification. If the prover has modified or deleted a substantial portion of F, then with high probability it will also have suppressed a number of sentinels.

Verification Phase:

The verifier before storing the file at the archive, preprocesses the file and appends some Meta data to the file and stores at the archive. At the time of verification the verifier uses this Meta data to verify the integrity of the data. It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted. It does not prevent the archive from modifying the data.



CONCLUSION

Finally we conclude that the concept of integrity was achieved in cloud storage with minimum amount of cost. Our proposed scheme reduces the computational cost and time.

Through the data integrity network bandwidth consumption are reduced .

REFERENCES

[1] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrityin outsourced databases,"Trans. Storage, vol. 2, no. 2, pp. 107–138, 2006.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searcheson encrypted data," in SP '00: Proceedings of the 2000 IEEE Symposiumon Security and Privacy. Washington, DC, USA: IEEE ComputerSociety, 2000, p. 44.

[3] Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for largefiles," in CCS '07: Proceedings of the 14th ACM conference on Computer and communications security . New York, NY, USA: ACM, 2007, pp.584–597.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable data possession at untrusted stores," in CCS '07:Proceedings of the 14th ACM conference on Computer and communica-tions security . New York, NY, USA: ACM, 2007, pp. 598–609

[5] Giriraj Chauhan,Sukumar Nandi: QoS Aware Stable path Routing (QASR) Protocol for MANETs, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[6] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)

[7] Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game theoretic Approach, in Proceedings of the 2nd ACM symposium on Information.

[8] S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

[9] Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim "DDoS flooding attack detection through a step-by-step investigation" 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications, ISBN: 978-1-4673-0495-5,2011

[10] Qi Chen , Wenmin Lin , Wanchun Dou , Shui Yu " CBF: A Packet Filtering Method for DDoS Attack Defence in Cloud Environment", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN: 978-0-7695-4612-4.2011.