www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 11 November, 2014 Page No. 9350-9354

Dynamic Data Storage for Trustworthy Cloud

Prof. M.M.More, Mahesh R. Bhujbal, Ashitosh K. Chourasiya, Balwantsingh D. Chauhan, Pankaj D. Pawshe

Project Guide
NESGOI,Pune
(Department of computer Engg.)
mrmukeshmore@gmail.com

NESGOI, Pune
(Department of Computer Engg.)
mahesh.bhujbal05@gmail.com

NESGOI, Pune
(Department of Computer Engg.)
ashitoshchourasiya10@gmail.com

NESGOI, Pune
(Department of Computer Engg.)
devrajsingh9767@gmail.com

NESGOI, Pune
(Department of Computer Engg.)
pankaj.pawshe99@gmail.com

Abstract:
The Side real Day many organization addresses problems nonstop growth of user huge increasing consumption of high performance of data storage. The dynamic data is very expensive and important to the organization and handle to that data organization needs very qualified or responsible people. Cloud service provider(CSP) offers the Lease facility for cloud model Storage -as- a-service which enables user to store his data in secured form on remote server. The Storage as service (SaaS) helps to reduce cost and maintenance level of organization end. Organization outsources their data on remote server to minimize the burden of huge local data and store on remote server. Data owner, Creates the specific level of security. If, any misbehavior by owner than it will pay for that to the CSP. Now a days, the Growth of cloud computing technology ratio also increasing in the world because of their security concern. Cloud computing many security issues related to securing data and examination of utilization of cloud by user. In this paper, We use the reliable Infrastructure of Cloud storage that provide the data owners all facilities offered by cloud and establishes the mutual trust between user and cloud.
The following four remarkable features offered by our proposed system:
1. It permitted owner to store dynamic and sensitive data and performance the full block level dynamic operation (i.e modification, insertion, deletion and append).
2. It permitted to registered user rights to access the owners files and latest version of updated dynamic data.
3. It permitted to owner having control the access of outsource data (i.e. grant & revoke control access) .
4. It establishes trust between the owner and cloud.

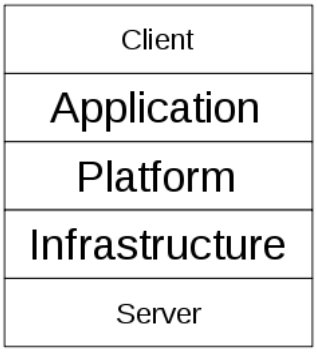
Introduction:

Cloud computing is a virtualized integrate power and storage provider via platform independence agnostic infrastructure of abstracted hardware and software access over the remote server. Cloud computing is a general term which provides the hosted services through the internet. These services effectively divided into three classes:

Infrastructure-as-a-Service (IaaS)
Platform-as-a-Service (PaaS)

Software-as-a-Service (SaaS)

To fulfill the it businesses and it operation to the expert. The name cloud computing was inspired by the cloud symbol that often used to represent the internet in flowcharts and diagrams.



Infrastructure as a Service (IaaS):

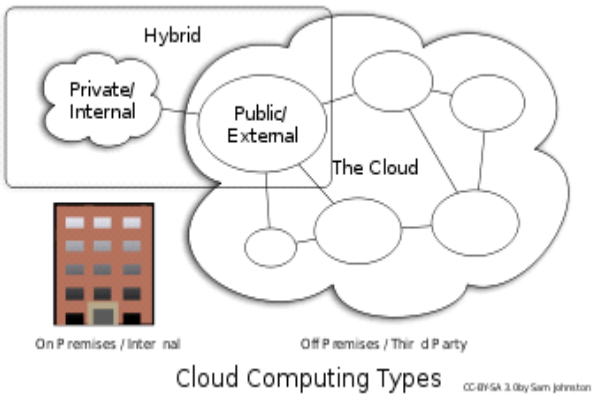
Infrastructure-as-a-Services like Amazon web services provides virtual server to instance Application Programming Interface (API) to start, stop and access control to the virtual server and storage. IaaS cloud the provide the resource on their dumpy on demnad.To deploy their application cloud user install as image and their application software on cloud. The cloud user maintains the operating system and application server.

Platform as Service (PaaS):

Platform-as-a-Service in the cloud is defined as set of software and product development tools. Developer creates application the provider's platform over the internet. The PaaS Infrastructure provide and their software solution an cloud platform without cost and complexity. Without purchase hardware and software .It provides the real-time cloud environment. Google app is example of Paas.

Software as Service (SaaS):

The Software-as-a-service cloud model provides the hardware infrastructure and the platform that run the application as internet with user through the front end portal. The SaaS has very popular market. It provide the remote service to inventory control and database processing. The host provided the both application and data to the end user free to use and remote access.



Public Cloud:

A cloud is called "Public cloud" because of its provided the network that is open for public use without any cost. public cloud provided offered on a pay-per-usage. The customer has no visibility over the location of the cloud computing.

Private Cloud :

A cloud is called "Private cloud" because of its computing architecture is dedicated to the customer and its not share with other organization. They are very expensive and more secured data than public cloud. In this significant signature requiring allocation of space hardware and environmental control.

Hybrid cloud:

A cloud is called Hybrid cloud" because of its combination of two or more cloud (i.e. Private, Public, Community) they are bound together. It is more secure private cloud and not secured in public cloud. The hybrid clouds the ability to collocation, managed and /or dedicated services with cloud resources. In hybrid cloud used "Cloud Bursting" to sharing the data as well as the resources to the other cloud. In this paper, the overview of outsource dynamic data storage. Data Owner represent the data storage and manage the data to a cloud in exchange for fix fees measured in GB/month. Using the remote server the owner stores the more data with help of outsourced data. The CSP providing the recovery facility of outsource data on multiuser server across, multiple data centers achieving higher level authority. The many registered users are allowed to remotely store that data cloud and access of that outsourced data. Owner physically stored the outsourced data and on cloud easily and maintain the same concern which is confidentiality, integrity and access control of control of the data. Example, In e-Health applications inside the USA the usage and exposure of protected health information should meet the policies admitted by Health Insurance Portability and Accountability Act (HIPAA) , and thus keeping the data private on the re remote storage servers is not just an option, but a demand. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers.

We purposed, the scheme that related the important issue related to the paper storage of data.

Data dynamic newness, mutual trust on cloud and user /owner access control on dynamic data.

The remotely stored dynamic data not only accessible for registered user but also the update and scalable user by the data owner. After updating the registered user must provide the updated data.

Our contribution is evaluated following two main classes:-

- It allows the data owner to stored data on CSP and perform the related operation which is fully block level(i.e. Modification, insertion, deletion and append the dynamic data)
- It provides the registered user only update data.
- It establishes the trust between owner and cloud to the help of Trusted Third Party(TTP).
- It enforces the access control for the outsourced dynamic data.

For example, in e-Health applications a physician may write a prescription based on a patient's medical history received from remote servers. If such medical data is not up-to-date, the given prescription may conflict with the patient's current circumstances causing severe health problems. Mutual trust between the data owner and the cloud is another issue, which is addressed in the paper. A mechanism is introduced to analyze the dishonest party, i.e. misbehavior from any side is detected and then the responsible party is identified. The access control is decided, which permitted the data owner to grant or revoke access rights to the outsourced dynamic data.

Related work:

In Existing research work can be found in the areas of cloud computing integrity verification of outsourced data, data storage security on entrusted remote servers and access control of outsourced dynamic data. The term cloud computing had already come into market in commercial use in the early 1990s to refer to large Asynchronous Transfer Mode (ATM) networks. By 21st century, he term ''cloud computing'' had allowed, although major focus at this time was on Software as a Service (SaaS). In 1999, sales- force.com was developed by Parker Harris, Marc Benioff. They applied many technologies of consumer web sites like Google and Yahoo! for the business applications. They also provided the concept's like ''on demand services'' and ''Software as a Service'' with their real business and successful customers. Cloud data storage (Storage as a Service) is an important service of cloud computing referred as Infrastructure as a Service (IaaS). Amazon's Elastic Compute Cloud (EC2) and Amazon Simple Storage Service(S3) are well known examples of cloud data storage. On the other side along with these benefits' cloud computing faces huge challenges i.e. data storage security problem, which is an important things of Quality of Service (QoS). Once user puts data on the cloud rather than locally, he has no control access over the cloud i.e. unauthorized users could modify user's data or destroy it and even cloud server attacks. Cloud users are mostly worried about the security and reliability of their data on the cloud. Amazon's S3 is such a good example.

Proposed System :

1. Owner

This is important module. Using this module owner get login to cloud system. Owner is able to upload data on cloud with master key. He have to authority to provide access of data to user .Owner assign new sequential key to user to access updated data.

2. User

This module is use to register new user. After login successfully user can access the data from cloud. Each time user get new key from owner to access updated data.

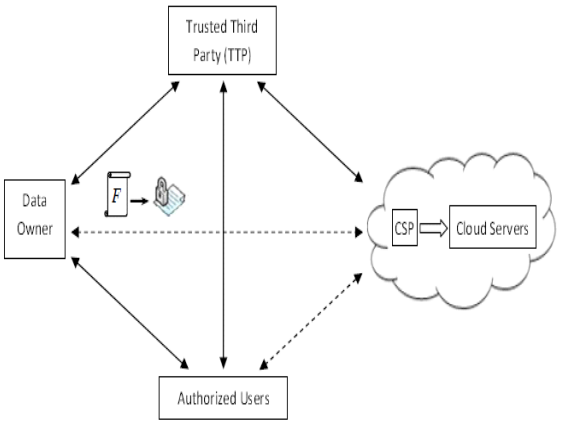
3. TTP

In this module TTP has monitors the whole working of this cloud system. Owner store data on cloud though TTP. TTP check for registered owner, TTP store new updated data on cloud with new access key, maintain the index for stored data, avoid unauthorized user from cloud, create sequential key for user. Broad cast new key to authorized user for access updated data.

4. CSP

In this module CSP has verify owner's key first. Then only CSP allows store the file in his cloud server. CSP is responsible for providing required hardware. CSP also responsible for protect data from any disaster. CSP take backup of whole data stored on cloud.

System Architecture :



Cloud service provider (CSP)

It is manages cloud servers and provides storage space on lease its infrastructure to store the owner's files and outsourced data to make them available for authorized users.

Authorized users

Its a set of owner's clients who have the right to access dynamic data by remote login.

Trusted third party (TTP)

It is entities which trusted by all other system components, and has capabilities to detect/analyze specify dishonest parties. . The relations between different system components are

Represented by double-sided arrows and solid and dashed arrows represent trust and entrusted relations between the component. For example, the data owner, the authorized users, and the CSP

trust the TTP. On the other hand, the data owner and the registered users have mutual entrust relations with the cloud. Thus, the TTP is used to enable indirect mutual trust between

these three components. There is a direct trust relationship between the data owner and the authorized users.

Data owner

That can be an organization / individual generating sensitive dynamic
data to be stored on the cloud and made available for access control to the registered user.

Algorithm :

In this system we used DES algorithm.

Problem Statement:

In this Project with DES algorithm three methods are mainly used to generate the key:

- Lazy Revocation
- Key Rotation
- Broadcast Encryption

In DES (Data Encryption Standard) algorithm CRYPTOGRAPHY is an algorithmic process of converting a plain text or clear text message to a cipher text or cipher message based on an algorithm that both the sender and receiver know, so that the cipher text message can be returned to its original, plain text form. In its cipher form, a message cannot be read by anyone but the intended receiver. The act of converting a plain text message to its cipher text form is called enciphering. Reversing that act (i.e., cipher text form to plain text message) is deciphering. Enciphering and deciphering are more commonly referred to as encryption and decryption, respectively. There are a number of algorithms for performing encryption and decryption, but comparatively few such algorithms have stood the test of time. The most successful algorithms use a key. A key is simply a parameter to the algorithm that allows the encryption and decryption process to occur. There are many modern key-based cryptographic techniques. These are divided into two classes: symmetric and asymmetric (also called public/private) key cryptography. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric key cryptography, one key is used for encryption and another, mathematically related key, is used for decryption.

Security requirements

Confidentiality- Outsourced data must be protected from the Trusted Thired Party, the CSP, and users that are not granted access.

Integrity- Outsourced data are required to remain interact on cloud servers. The data owner and registered users must be enabled to recognize dynamic data corruption over the CSP side.

Conclusion:

Finally, Cloud computing is a simple idea, but it can have a huge impact on your business. the owner is capable of not only archiving the files and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The Owner every time provide the updating dynamic data to the registered user. It provides the more security to the dynamic data.

Future scope:

- In the Cloud system we use the biometrics authentication of the authorization of user for more security.
- In the cloud computing Grid Computing was the last research-led centralized approach.
- In the cloud computing there are adoptions of cloud computing could cause many problems for users.
- There are many new open source systems appearing that you can install and run on your local Infrastructure should be able to run a different of variety of applications on these systems.

Reffrences:

- Ayad Barsoum, Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems", *IEEE Transactions on Parallel & Distributed Systems*, vol.24, no. 12, pp. 2375-2385, Dec. 2013, doi:10.1109/TPDS.2012.337

- A. Singh and L. Liu, "Sharoes: A data sharing platform for outsourced enterprise storage environments," in Proceedings of the
24th International Conference on Data Engineering, ICDE.

- IEEE, 2008, pp. 993–1002. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," Online at http://aspe. hhs.gov/admnsimp/pl104191.htm, 1996.

- 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 Communications Security, New York, NY, USA, 2007, pp. 598–609.

- Y. Deswarte, J.-J. Quisquater, and A. Sa¨ ıdane, "Remote integrity checking," in 6th Working Conference on Integrity and Internal Control in Information Systems (IICIS), S. J. L. Strous, Ed., 2003, pp. 1–11.

- D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data

transfer," Cryptology ePrint Archive, Report 2006/150, 2006.

•E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," Trans. Storage, vol. 2, no. 2, 2006.

•F. Seb´ e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. and Data Eng., vol. 20, no. 8, 2008.

•M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in HOTOS'07: Proceedings of the 11th USENIX workshop on Hot topics in operating systems, Berkeley, CA, USA, 2007, pp. 1–6.

•M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.