ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 3, March 2016

A SECURE WITH EFFICIENT DATA TRANSACTION IN CLOUD SERVICE

DR.C.K.GOMATHY[1], V.GEETHA[2], S.MADHUMITHA [3], S.SANGEETHA[4], R.VISHNUPRIYA[5]

[1&2]Assistant Professor- Department of CSE, SCSVMV

[3, 4, 5] UG Scholar, SCSVMV University, Kanchipuram, Tamilnadu, India.

***ABSTRACT*:**

The software programs run from the systems. Data hiding is an secret information in a effective control with its original content and it's stored on servers accessed via the Internet. It denotes a major change in how its stored information and run applications. Instead of running programs and data on a systematic manner, everything is hosted in the cloud and servers access via the internet. An environment created in a user's machine from an online application stored in a cloud and run through a web browser. Security issues are becoming the major drawback of cloud. In previous work, security problems originate from Loss of control, Lack of trust,multi-tenancy.In this paper elaborates, the users are connected to the cloud through the internet and the primary and secondary keys are generated for data sharing, and the files can be encrypted by using merkley hash tree algorithm. if the user wants to download the files user have to ask permission from the data owner ,only if the user is authenticated then the mutual key can be shared by the data owner in the form of steganography ,so the user trust and seclusion is achieved

Keywords: **Secure Transactions, Quality of Cloud Service, Pattern Transactions, Pairwisekey Management, Steganography.**

I. INTRODUCTION

Cloud Computing has been anticipates as the next generation architecture of IT Enterprise. It's not the technology it is one of the computing model. Cloud computing gives financial benefits to the organization as well as the clients, because they should pay the money only depends on the usage of the services. Cloud computing is the delivery model of cloud services over the internet.Cloud provides all of its initiatives as services, the most famous services as Software as a service(Saas),Platform as a service(Paas),Infrastructure as a service(Iaas).Saas:A single application is delivered to the group of users from the vendor's server, the user can access the application through Application Programmer Interface(API).Paas:The development framework is offered as a service.Iaas:The third party will provide the hardware services to the users. The main qualities of cloud transaction computing are:

- *Lower Software Cost*
  There's the problem of software cost. Instead of buying separate software for each computer, only those who need the application can access and utilize it.

- *Instant Software Updates*
  The users are not forced to use the same features of the particular application can upgrade the software.

- *Universal Access to Documents*
  Anywhere you can access the documents, if you have a constant internet connection.

- *Latest Version Availability*
  If the user wants to edit the document many versions are available for the user purpose.

The Problems of cloud transaction is

- *Less Security*
  The information stored in the cloud could not be secure, there is a chance of several attacks, so the files might be not secure.

- *Needs a Constant Internet Connection*

The users should have persistent internet connection, and then only users can able to access the cloud.

- *Can be Slow*
  Even in a fast connection, some web applications can be slower than accessing the homogenous software programs in pc.

II. RELATED WORKS

The idea a good person may remotely accessibility their own data throughout on demand mode. plus the diversity of an application requirements, users will probably want to be able to entry along with share each other's authorized details fields to be able to achieve productive benefits, which delivers new security and privacy challenges with regard to the cloud storage [1].The concept of cloud computing is acquiring a lot of recognition from both academic and business worlds. The main idea is to make claim obtainable on adoptable execution framework primarily located in the internet.In cloud computing, users can outrace their computation and storage to servers using internet [2]. Cloud computing's multi-client feature, which provides distinct, seclusion and access control challenges, because of sharing of resources among unbelievable clients [3]. In Cloud computing, a third party is responsible for providing, processing power, memory space and implementation support etc. Cloud database is maintained by third party Cloud provider, so user hesitates to keep his data at cloud database [4].

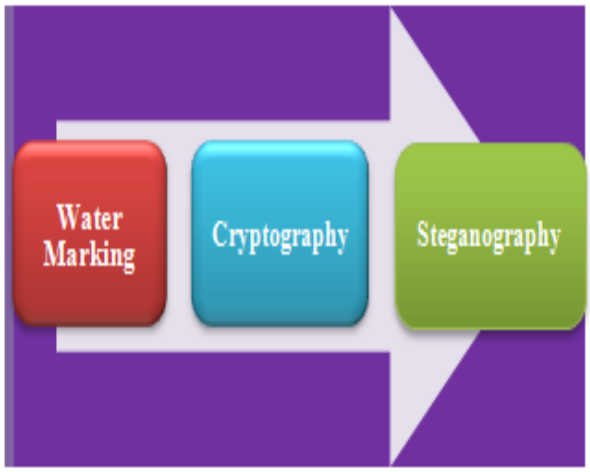

Fig 1: Generating Secure Technology

III. FEATURES OF SECURE DATA TRANSACTION

3.1 Multi-Aspect Authentication

A number of cloud computing vendors offers multi aspect authentication as part of the service. It is more secure than traditional use and name password convention.

3.2 Security Patching

The software products that we use today requires rigorousness when it comes to applying security patches and testing this patches to make sure they were properly applied.

3.3 The cloud offers economies of scale

Due to the rife of IT and the essential role it plays in running the business, it make sense to view IT as a ideality ,rather than dedicated capability.

3.4 Physical security

Cloud computing vendors host the system in facilities that have much better physical security control with valuable certification that many small to large companies cannot provide on their own.

IV.IMPLEMENTATION TECHNIQUE

In this research work contributed, an Access key is generated while Registration with Cloud. After that only Shared Keys are generated. Finally a Mutual Access key is generated by the data owner to the data user and sent via Email. Data User will have to hide that Mutual Key in an Image called Steganography and sent to the Data Owner. Data is accessed by only after Verifying Mutual Key using Destaganography.The following terms are the techniques used to implement:

i) The User want to create an account, then only they are allowed to access the cloud, initially the user have to register in the login page.

ii) The Service provider will manage the all the User information to authenticate the User when are login into their account.

iii) The verifier will generate the signature using change and response method.

iv) Access key is generated to access the data, after that if you want to share it will provide the shared key for getting access from the cloud owner.

v) The cloud users want to access the files like download, then he/she has to get the permission from

the cloud owner, the cloud owner will verify the mutual key.

vi) The cloud user to interact with the cloud owner. so in this caliber the user will search the files that is end user can search the files but he cannot see the file because they need to get permission from the cloud owner by using the mutual key, and to share data validate the shared key.

Fig 2: Principles of Steganography

vii) The fundamental concept of steganography is that message to be transmitted is not noticeable to casual eye.

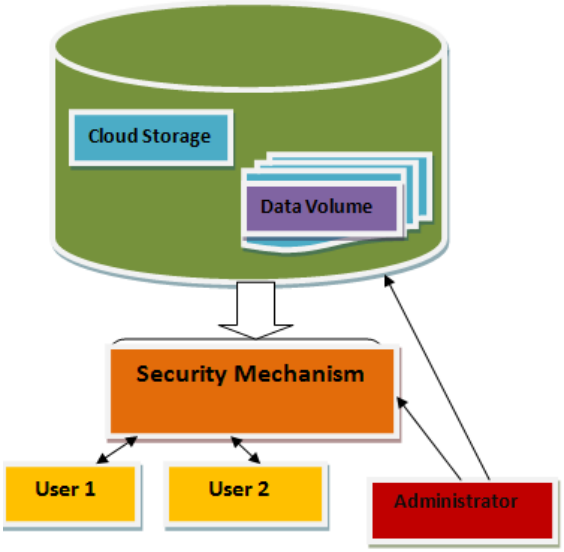

Fig 3: A Scheme of Security System

The model of cloud storage composed of four layers: storage layer which saves the data, basic management layer which enable security and solidness of cloud storage itself, application interface layer which provides application platform and access layer which provides the access platform. The public data is sharable among authorized clients that provide an open framework for collaboration. Private data is client's secured data that must be transmitted in cipher form for security and privacy.

v. CONCLUSION

In this research proved, data loss, lack of trust, data security is overcome by using steganography technique. The verifier can take care of user's information, so various attacks can be avoided. The user is authenticated and authorized, insider threats can be identified and abstrained.Data affinity and integrity is achieved. This property of hiding information is highly describable for military, business sector and IT organization.

VI. REFERENCES

[1] Rudresh Bagade and C.R.Barde,"Multi-user Data Sharing Authentication Protocol for Cloud Computing with Seclusion",2015

[2] S.Divya Bharathy and T.Ramesh,"Securing Data stored in clouds using privacy preserving authenticated access control",2014

[3] R.Ranjith and D.Gayathri devi,"Secure cloud storage using Dcentralized access control with anonymous authentication",2013

[4] C K Gomathy,"Cloud Computing: Business Management For Effective Service Oriented Architecture" International Journal Of Power Control Signal And Computation (IJPCSC) Vol. 1 No. 4 ISSN : 0976-268X,2010.

[5] Pradnyesh Bhisikar and Prof. Amit Sahu "Security in Data Storage and Transmission in Cloud Computing",2013

[6]Keiko Hashizumer, David G Rosado Eduardo Fernández-Medina and Eduardo B Fernandez," An analysis of security issues for cloud computing",2013

[7] Maninder singh and sarbjeet singh,"Design and implementation of multi-tier authentication scheme in cloud",2012