Third party auditor in cloud computing (survey)

Mrs. Mala dutta
Asst.Professor, Dept. Of computer engineering,
Institute Of Engineering & Technology ,
Devi Ahilya University, Indore, India.

Mustafa khan
Dept. Of Computer Engineering ,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

Abstract :-

In an October, 2009 presentation titled "Effectively and securely using the cloud computing paradigm" by Petter Mell and Tim Grance of the National institute of standards and technology (NIST) Information Technology Laboratory, cloud computing is define as follows:

Cloud computing is a model of enabling convenient, on demand network access to a shared pool of configurable and reliable computing resources(e.g., networks, servers, storages, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.

In this paper we are using third party auditor (TPA) for cloud.

Keywords- cloud computing, TPA.

Introduction:-

Cloud computing is the next generation platform to provide resources as the services to the end users. In cloud storage system, the clients store their data in the server but when storage expansion is needed they move to public clouds. Cloud Computing gained intention since 2007.It is the general term for anything that involves providing services on internet. It moves the data and computing from desktop to large data centers. Many big companies such as IBM, Google, Amazon, Microsoft, Yahoo and other move themselves to develop Cloud Computing.

MODELS-

- Delivery Models
  - SaaS (software as a service)
  - PaaS (platform as a service)
  - IaaS (infrastructure as a service)
- Deployment Models
  - Private cloud
  - Community cloud
  - Public cloud
  - Hybrid cloud
- We propose one more Model: Management Models
  - Self-managed
  - 3rd party managed (e.g. public clouds)

- Saas- Application that is deployed over a network, typically the web, accessible via a browser or program interface; referred to as software on demand.
- Paas- A platform on which user can build application using languages, libraries, services and tools supported by the provider.

Iaas- Processing and storage capacity, networking and computing resources where the has control over operating system and deployed application; sometimes referred to as utility computing.

Literature Survey :-

This section provides the study on the recent contribution placed in the domain of hybrid cryptographic data models.

According to Renuka Goyal, Navjot Sidhu[1] exist "Cloud computing provides many benefits to their user but security is major issues in cloud computing. As user store their data to cloud data centers but as user does not know the exact location of their data so integrity of data is very important. To check the integrity of data there are many solutions available. One of solution is to take the assistance of a third party auditor. Different authors provide different solutions for implementing third party auditor.

According to Ashish Bhagat and Ravi kant Sahu [2]

Conclude that secure auditing protocol to store data and verify it and make algorithm with example. Use the RSA algorithm with ElGamal Digital Signature and for the process of encryption and decryption and which is solve the problem of integrity, unauthorized access, privacy and consistency. And in this article first present a network in which cloud Architecture work and which methodology used, user and TPA shown after that how file is retrieved.

According to D.C. Chou [3]The rise of cloud computing is closely related to the increasing practice of information systems outsourcing. We first discuss the practice of information systems outsourcing.

We first discuss the implication of information systems outsourcing. Information systems outsourcing is an important practice in business operation, which hires outside IT professional services to meet a company's in-house needs.
Business process outsourcing (BPO) has been integrated into corporate management as an organizational strategy[2].

According to (Patel & Patel, 2012) (Gowrigolla, Sivaji & Masilliamani, 2010) (Balakrishnan et al, 2011) [4] standard - TPA in cloud environment should take following functionalities into consideration:
1) No data leakage or data learning: TPA should neither learn any information about the data file from the message it receives from client/server nor leak the same to any unauthorized entity.
2) Audit without downloading: The TPA should audit without asking for entire file from server, not even in encrypted form. TPA should audit the user data without asking for the local copy of the data or even learning the data contents.

3) Integrity Verification: One of the important security concerns is to verify integrity of data stored on cloud. TPA should verify the integrity of client's data stored on cloud with low communication overhead.

4) High Performance: Performance of TPA is also an important issue as it is a central component of the cloud system, where there are thousands of client and multiple servers. TPA should not become bottleneck of entire system and performance of overall system should not be compromised due to heavy load on TPA.

5) Scalability: As cloud is a completely dynamic environment, any number of users can come in or go out.
Also it is expected to have huge data storage on cloud server. Functionalities of TPA should not be affected by number of cloud clients, servers, number of data files stored on the cloud or the overall size of the entire storage. TPA should offer scalable architecture which is independent on all the factors mentioned.

Security issue :-

The most important issue is that a user needs to manage multiple private keys learned from each service provider. To resolve user key management issue ,the simplest way is that all service providers share the same master private key. However, if an adversary attacks one of the service providers successfully, he/she can learn this master private key and masquerade as any one of the service providers to cheat users. In addition, a malicious adversary, who has obtained the master private key from a service provider, can learn session keys established between another service provider and a user if the applied authentication scheme does not support perfect forward secrecy[7].

When two or more users are using data any time then consistency of data is more important because unauthorized person can use data and it can change or modify data or delete the data. New data storage paradigm in cloud computing bring about many challenging design issues which has deep effect on the performance and security of overall system.

- It may be possible that an unauthorized user can access the data from the public clouds. Hence, it is of critical importance that the client should be able to verify the integrity of the data stored in the remote un-trusted server.
- There may be security services offered by public clouds but they are not sufficient.

In order to address the security issues, Trusted Third Party Auditing (TPA) is used as a service for private and public clouds, which offers various services to check for the integrity of the data .

- On the other hand the security in the Cloud computing system having some lacks which is desired to improve are listed below:
- **Less secure authentication technique:** the authentication system consumes weak attributes for performing end client authentication, therefore security during authentication management is poor, thus desired to improve the authentication technique.
- **Computationally expensive cryptographic approach:** the implemented cryptographic techniques are computationally week and consume higher space and time complexity for encrypting fewer amounts of data.

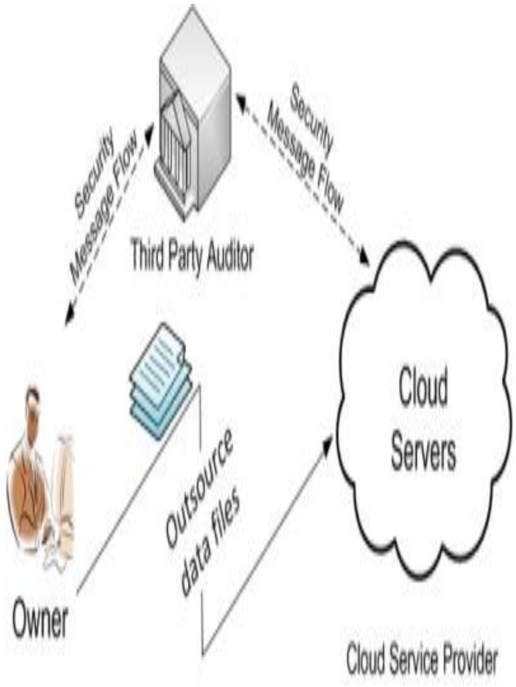
Proposed work:–

A Third Party Security Auditor proposed to provide higher security with less concern management.

- The main goal of this paper is to provide introduce third party security server for genuine evaluation of security level.

Third party auditor-

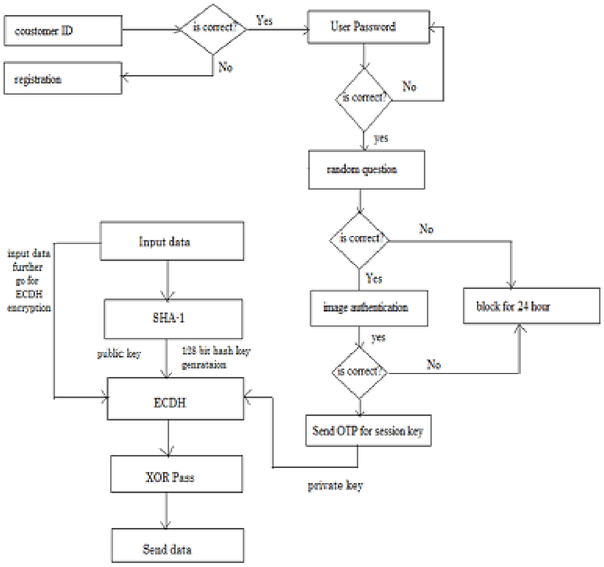
- The Third party auditor is a kind of inspector. The Third Party Auditor who has resources and experience that a user does not have and check the integrity that is difficult for users to check.



According to Miss. Nupoor M. Yawale & Prof. V. B. Gadichha [5]

Third party Auditor (TPA): Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing.

“The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an un-trusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a Trusted Third Party Auditing (TPA), which offers its auditing service with more powerful computation and communication abilities. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. [6]



The proposed working model and their involved processes are given in the above diagram, in this diagram a number of sequencial processes are taken place.

- ❑ First user provides their ***customer ID*** for initializing the authentication process if user is not registered then system redirected to the user for ***registration process***.
- ❑ If customer id found in database user go to next step for password. Than check password and if password wrong than go to previous step otherwise go to next step which is system generate random question which is submitted previously during registration process.

Future work :

- ➢ if login ID is connected with new m/c or network then OTP is gernated.
- ➢ if login ID is connected to same IP or n/w which was used once, then there is no need to OTP password.

Conclusion –

This paper has proposed a new anonymous authentication scheme.

- ✓ Cloud computing is broadly accepted in the IT industry. Its development brings in benefits such as cost saving, ease of use, scalability, flexibility, and environmental sustainability.
- ✓ Cloud computing provides many benefits to their user but security is major issues in cloud computing.

` REFRENCE-

[1]Renuka Goyal, Navjot Sidhu Renuka Goyal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4526-4530

[2] Ashish Bhagat and Ravi kant Sahu *International Journal of Computer Applications (0975 – 8887) Volume 70– No.16, May 2013*

[3] D.C. Chou, An investigation into IS outsourcing success: the role of quality and
change management, Int. J. Inf. Syst. Chang. Manag. 2 (2) (2007) 190–204.

[4] (Patel & Patel, 2012) (Gowrigolla, Sivaji & Masilliamani, 2010)
(Balakrishnan et al, 2011)

[5] Miss. Nupoor M. Yawale & Prof. V. B. Gadichha, (Volume 3, Issue 11, November 2011 ISSN: 2277)(International Journal of Advanced Research in Computer Science and Software Engineering)

[6] Anne Srijanya. K, N. Kasiviswanath International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013

[7] Jia-Lun Tsai and Nai-Wei Lo, IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015.