Implementation and Design of Mechanism using by Third Party Auditor for Security in Cloud Computing

Monisha Chauhan[1] Dr. Mamta Bansal[2] Dr. R.P. Agarawal[3]
[1,2,3]Department of Computer Science
[1,2,3]Shobhit University, Meerut

Abstract— Cloud Computing is a computing where many people throughout the world are connected to private or public networks. It is internet based computing through which we share data along with various services also. The main and important concerns about the cloud storage services are authorization and trust management for the cloud service provider (CSP).Third Party Auditor (TPA) plays important role to achieve these problem. TPA has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage security. In this paper we give and discuss about few emerging trends in cloud computing as well as we proposed a new model i.e. Intelligent Third Party Auditor(ITPA).This model used various technique like compression, encryption ,Meta data with all related operation(Insertion, Deletion, Update) .This proposed model are introduced for confidentiality, integrity and access control for cloud storage systems. This proposed model also reduced computational and communication cost between CSP and User as well as between User and TPA. We are trying to propose here soft computing by taking pattern recognition in Robust Module.

Key words: Cloud Computing, Third Party Auditor(TPA), Cloud Security, Cloud Service Provider, Encryption Technique, Compression Scheme, Computational cost, Communication cost

I. INTRODUCTION

Cloud Computing is concerned with the sharing and vision of computing as utility, where data is centralized or outsourced into the cloud. It also appear as a computational model as well as distribution architecture and its main purpose is to give secure , quick ,convenient data storage and net computing service, with all computing resources visualized as services and delivered over the internet.. These services are broadly divided into three categories:

Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

A. Infrastructure-as-a-Service (IaaS):

The potential provided to the user 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 system and application

B. Platform-as-a-Service (PaaS):

This service provides the potential to the user to deploy on top of the cloud infrastructure his own applications without installing any platform or tools on their local machines. It refers to providing platform layers resources, including operating system support and software expansion frameworks that can be used to construct higher-level services.

C. Software-as-a-Service (SaaS):

In this service user 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.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

II. LITERATURE SURVEY

Many diverse factors such as integrity of data, data dynamics and data privacy affects the performance of a number of approaches in cloud data storage. Each and every approach has merits and demerits which make them suitable for different applications. TPA play main role in the integrity and validating of data. For well organization it is very essential that cloud that allows investigation from a single party audit the outsource data to ensure data security and save the user's computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party auditor (TPA). TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable way for users to check the validity of data in cloud. In this literature survey we discuss different approaches which are already carried out for cloud data security [7].

A. Digital Signature using RSA:

K.Govinda, V.Gurunathaprasad, H.Sathishkumar [1] proposed a method in which RSA algorithm used for encryption and decryption which follow the process of digital signature for the message authentication. There are three main participants.

- Third Party Auditor (TPA)
- User
- Cloud Provider.

User and the TPA generate their own private key and public key with respect to the strong RSA algorithm. The public keys have been shared between them as the part of SLA or in some other ways. Then with respect to the protocol the message is encrypted as well as signed in a unique way.

B. Virtual Machine used with CU and TPA:

A.Mohta, R.K.Sahu, L.K.Awasthi[2] proposed Virtual Machine which uses RSA algorithm, for client data/file encryption and decryptions. SHA 512 algorithm is also used which makes message digest and check the data integrity. The digital signature is used as an identity measure for client

or data owner. Problem of integrity, unauthorized access, privacy and consistency are also solved in this proposed system.

C. Privacy Preserving Public Auditing:

Cong Wang proposed public auditing[3] that allows TPA along with user to check the integrity of the outsourced data stored on cloud and Privacy Preserving allows TPA to do auditing without requesting for local copy of the data and cloud data privacy is maintained. In this process we have following algorithms:

- Keygen
- Singen
- GenProof
- Verifyproof

In Keygen, a key generation algorithm used by the user to setup the scheme. Singen algorithm used by the user to generate verification metadata which may include digital signature. Genproof algorithm used by the Cloud Server to generate a proof of data storage correctness. Verifyproof used by the TPA to audit the proofs. With the help of this scheme, TPA can audit the data and cloud data privacy is maintained. It is divided into two parts 1) Setup Phase and 2) Audit Phase and its methodology. TPA checks the integrity of the outsourced data stored on the cloud without accessing actual contents.

D. Privacy Preserving Public Auditing with Watermark Process:

T.Paigude and T.A.Chavan[4] proposed a system in which they used water marking process, to store the data or images in the cloud server by assigning the public key and this key and watermarking images are sent to third party and third party have complete authority to check the key and sent it to the server, and there TPA must have a public key whenever the data is retrieved. In this process, the security level is very high and due to this the data or image cannot be identified by the attackers in the cloud.

Watermark information is embedded into original image itself, and it is performed in the encryption process for making security on original information. With the help of this technique, cloud data storage will be more protected.

E. Service Level Agreement (SLA) between Cloud and Customer:

Vinaya.V and Sumathi.P[5] provide a scheme which checks data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. But this can be agreed upon by both the cloud and the customer and can be incorporated in the Service Level Agreement (SLA). They presented a model for secure integrity verification scheme and with data update protocol that dynamic data modification by introducing effective TPA. They addressed two main issues: Data correctness and Public auditability. Data correctness means that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users data intact. Public auditability is to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

F. Monitoring Data Integrity while using TPA

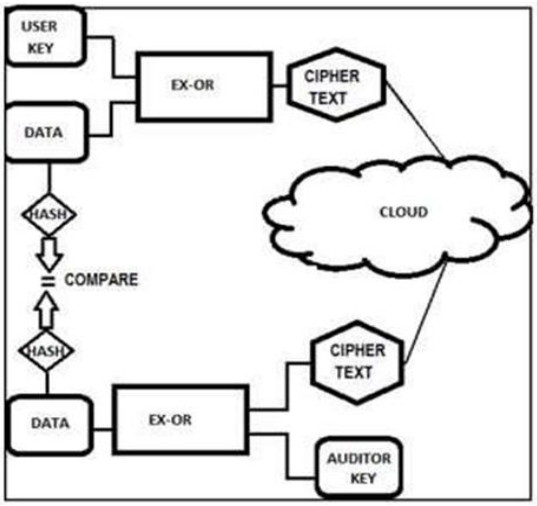

Fig. 1: Methodology

Jaspreet K and Jasmeet Singh proposed[6] scheme using SHA-2 which is cryptographic hash function to verify the integrity of data along with XOR mechnasim, Station-to-Station key protocol for key generation and mutual authentication with TPA. For ensuring the integrity of data ,following three approaches are used and it is also explain with the help of above diagram [Fig. 1]:-

1) Station–to-Station protocol:

It generate mutual key which is known to both user and auditor and provide entity authentication to both.

2) Exclusive-OR (XOR):

It performs xor operation between the message and key generated using Station-to-Station protocol.

3) Secure Hashing Algorithm

It is used generate a digest by passing the original message to hash function. After doing this, the value obtained by both the user and the auditor are compared and hence the data integrity is verified.

III. PROBLEM IDENTIFICATION

Existing system in Cloud computing providing unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are just accessing or renting; they can forego capital expenditure and use resources as a service, paying instead for what they use.

- Benefits of Cloud Computing:
- Minimized Capital expenditure
- Location and Device independence
- Utilization and efficiency improvement
- Very high Scalability
- High Computing power

As we know that the user's data are stored in data centre's, which are remotely located. In these techniques clouds have more security challenges which need to be clearly understood and resolved. One of the major concerns with cloud data storage is that of data integrity verification at un-trusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the advantage of their personal. TPA (Third Party Auditor) have proposed many algorithms as we mentioned in literature survey above. We also agree that it works but still

we find lots of problems in security area in cloud computing. In the existing system TPA has the following drawbacks:

- TPA demands retrieval of user data, here privacy is not preserved
- TPA have to remember which key has been used
- These two schemes good for static data not for dynamic data

Present study suggest to develop new algorithms for removing the security problems which comes in cloud computing like Data centre Security, Network Security, How secure is encryption Scheme etc which depend on the TPA.

Concise problem statements:

- Problem of encryption
- Reduce workload on server
- Use of others hard disk space effectively
- Reduce cost of server
- Less fault tolerance
- File System running on all type of computing

IV. PROPOSED WORK

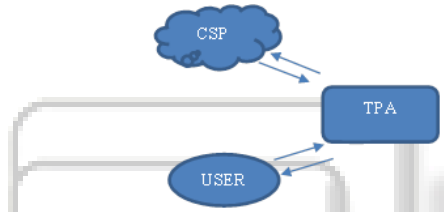

Fig. 2: Cloud Computing

Key Elements of ITPA are

A. CSP (Cloud Service Provider):

The work of CSP is same as ever that it offers customers storage or software services available via a private (private cloud) or public network (cloud). Generally, it means the storage and software is available for access through the Internet.

B. ITPA (Intelligent Third Party Auditor)

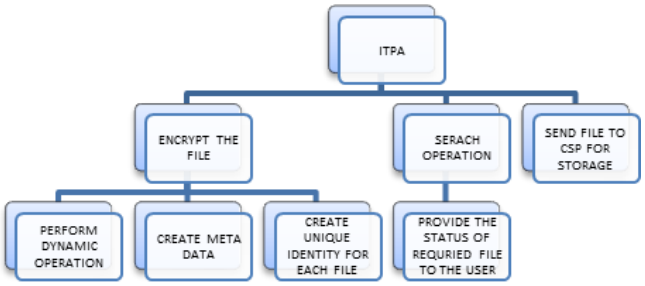

Fig. 3 Advanced Mechanism of Intelligent Third Party Auditor

Basically all above work is done by the ITPA. The important thing is important here it reduce the workload on CSP as well as on User. Here user can be trusted completely on ITPA because CSP is used only for storage and all rest work can be done through ITPA. Availability of file or data on cloud is also be achieved here. Technically all concerned algorithms of this work will be given in further work.

C. User:

User can be trusted on ITPA due to its architecture. In our proposed work before going to ITPA file should be passed through a module i.e. Robust Module. The work of this module is:

- Compress the file
- Taking thumb print of user
- Size of compressed file
- Add some important changes to the size of compressed file
- Send it to the ITPA

All these work can be performed by this RM. For the security purpose it should be achieved. We proposed such module for more security as well as for checking the authenticity of ITPA.

Cloud computing give us resources in the form of service rather than a product, utilities are provided to the users over internet. The main goal is to secure, protect the data and the processes which come under the property of users. It is an special and important research area which requires lots of development from both the academic and research communities. In cloud computing, all resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data.

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. We proposed secured cloud storage system, by using new security algorithm and maintain the integrity of outsourced data in cloud environment. In the cloud, all data and services are exist in centralized huge data center, which is not easy to handle and not-trustworthy. Our aim is, to design efficient and new mechanism using different techniques with the help of TPA (Third Party Auditor) for data verification and operation and achieve the following goals and also remove the above mentioned drawbacks:-

- Storage should be correct and kept intact (complete) all the time in the cloud.
- Data is dynamically available with assurance of data accuracy even if data is modify, delete or appended by the user in the cloud.
- Accountability in cloud data - trustable, reliable and customers should be satisfied.
- Privacy of user data is highly secured.

In the above mechanism of intelligent third party auditor, all file / data should be stored in CSP through ITPA. At the start, files are sending through the ITPA and follows different techniques like Compression, Encryption and creates metadata about the encrypted file and then sent the file to the cloud server for storage. Metadata should be stored on ITPA as well as one copy should also be send to the user for further query, if needed. In this proposed work data is compressed with arithmetic coding technique which is not yet applied before in any model of cloud computing. Data is highly secured in this proposal and kept intact also.

V. CONCLUSIONS

Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Various

schemes are proposed by authors over the years to provide a trusted environment for cloud services. Encryption and Decryption algorithms are used to provide the security to user while using third party auditor. This study give us a brief view of different schemes proposed in recent past for cloud data security using third party auditor. Most of the authors have proposed schemes which rely on encrypting the data using some encryption algorithm and make third party auditor store a message digest or encrypted copy of the same data that is stored with the service provider. The third party is used to resolve any kind of conflicts between service provider client. The detailed security and performance analysis shows that the system is highly efficient and flexible to malicious data modification attack and reduces the external threats imposed over the cloud storage with the help of TPA. But we want to resolve all security problems with the help of TPA in highly secured way. So we want to proposed a new mechanism of TPA in cloud computing for ensuring the correctness and integrity of data in cloud storage. We will use compression techniques as well as metadata along with dynamic operation effectively, which makes this system more secure as comparatively other ones.

REFERENCES

[1] K.Govinda,V.Gurunathaprasad and H.Sathiskumar, "Third Party Auditing For Secure Data Storage in Cloud Through Digital Signature using RSA", International Journal of Advanced Scientific & Technical Research, vol. 4, issue 2-Aug 2012.
[2] A.Mohta and L.K.Awasthi,"Cloud Data Security While Using Third Party Auditor", International Journal of Scientific & Engineering Research, vol 3, issue 6-June 2012.
[3] C.Wang, Sherman S.M.Chow, Q.Wang,K.Ren and W.Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE Transaction on Computer I,vol.62,issue 2-Feb 2013.
[4] T.Paigude and Prof. T.A.Chavan,"A Survey on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Computer Trends & Techniques, vol.4,issue 3-2013.
[5] V. Vinaya and P. Sumathi," Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering,vol.3, issue 5-May 2013.
[6] J.Kaur and J.Singh,"Monitoring Data Integrity while using TPA in Cloud Environment", International Journal of Advanced in Computer Engineering and Technology, vol. 2,issue 7-July 2013.
[7] Bhagat et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(3), Volume 3, Issue 3-March 2013.

