A Survey over the Various Techniques Which used for Security of the Data in Cloud Storage

Avinash Shukla
M.Tech, Dept. of CSE
UIT, RGPV
Bhopal, India

Sanjay Silakari, PhD
HOD, Dept. of CSE
UIT, RGPV
Bhopal, India

Uday Chourasia
Assistant Professor,Dept. of CSE
UIT, RGPV
Bhopal, India

ABSTRACT
In recent time cloud computing provides an enhanced mechanism to access and share data which contain useful information, but that data stored in third party cloud server. Security of that data is the biggest issue in cloud computing. There are various techniques presented by the researchers to deal with such issues. There are techniques like privacy preserving techniques public auditing based techniques, batch auditing based techniques and some other techniques are used to provide authentication and provide security for the data in cloud storage. A review over the various techniques which used to provide security for the data over cloud storage is presented in this paper. For future work an enhanced technique for security can be proposed to deal with such problems.

Keywords
Cloud Storage, Cloud Security, Encryption, Decryption. Third Party Server (TPA), Redundant Array, Homomorphic function.

1. INTRODUCTION
Cloud computing is an emerging area of research which provides on demand services to the user called platform as a service, infrastructure as a service, software as a service, a standard architecture diagram for the cloud process is presented in Figure 1.1. In platform as a service (PaaS) development platform to the user is provided by the cloud service provider. That platform contains all the things like operating system, development environment for programming language etc. In infrastructure as a service (IaaS), physical resources or virtual resources are provided to the user to perform their tasks. There are vendors like Oracle, VMWare, Hyper-v, etc. In software as a service (SaaS) various software resources are provided to the user to perform their operations. There are various software or on-demand software resources are provided to the user need to pay as per their use.

There are generally three type of cloud are there in cloud deployment model, called public cloud, private cloud, hybrid cloud.

Public cloud

A cloud is consider to as a public cloud, if it provides service to the in open to all manner. Generally these services are provides free access to the user.

Private cloud

Private cloud is a cloud which provides services within an organization. These services can be managed internally or by a third party. There are various access levels or degree is defined for the users to access these cloud services.

Hybrid cloud

Hybrid cloud is the combination of the private and public cloud or public and community cloud etc. in that cloud all cloud having their own integrity but still bound together to provide on-demand services to the us

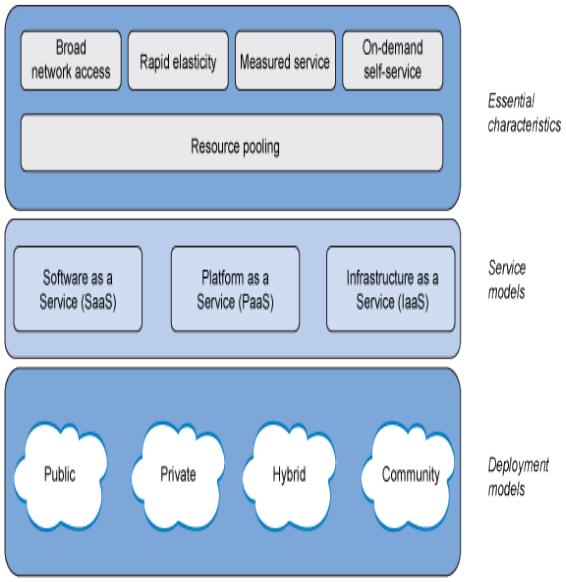

Figure 1.1: Cloud Architecture Diagram.

Figure 1.2: Cloud Storage Architecture.

Cloud storage may be a model knowledge of information storage within which the digital data is hold on in logical pools, the physical storage spans multiple servers (and usually locations), and therefore the physical setting is usually closely-held and managed by a hosting company. These cloud storage supplier square measure liable for keeping the info offered and accessible, and therefore the physical setting protected and running. Folks and organizations get or lease storage capability from the suppliers to store user, organization, or application information.

Cloud storage services is also accessed through a co-located cloud pc service, an internet service

Application programming interface (API) or by applications that utilize the API, like cloud desktop storage, a cloud storage entranceway or Web-based content management systems.

An architecture for the cloud storage in cloud computing is presented in Figure 1.2. That shows data from the various resources is stored in the cloud storage. Thus that data requires a secure mechanism to preserve privacy of the data.

A cloud storage framework provides by the various vendors is presented in Figure 1.3. That shows how data can be stored at various cloud servers, that framework provides an overview of the cloud storage framework.

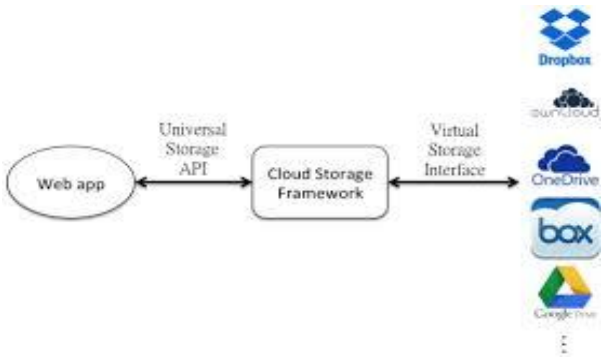

Figure 1.3: Process of Storing Data in Cloud Storage.

Benefits of cloud storage

Cloud storage may be a model knowledge of information storage within which the digital data is hold on in logical pools, the physical storage spans multiple servers (and usually locations), and therefore the physical setting is usually closely-held and managed by a hosting company.

These cloud storage supplier square measure liable for keeping the info offered and accessible, and therefore the physical setting protected and running. Folks and organizations get or lease storage capability from the suppliers to store user, organization, or application information.

Cloud storage services is also accessed through a co-located cloud pc service, an internet service application programming interface (API) or by applications that utilize the API, like cloud desktop storage, a cloud storage entranceway or Web-based content management systems.

In cloud computing user's data resides in third party server, which is vulnerable to the attacks and various security threats. To provide securityfor that data there are various techniques are presented by the researchers. But these techniques are still required some enhancement to provide on-demand services to the user. There are techniques like [3] an integrity verification scheme to provide secure storage over cloud is presented, which preserve the integrity of the cloud content. In [4] a data auditing scheme which uses privacy id based technique to provide privacy preserving the data in cloud storage. In [7] a privacy preserving technique which uses a share authority based privacy preserving protocol is presented which provides security for the data in cloud storage. In [10] a multi owner based technique for secure data sharing over cloud is presented, That provides a sharing mechanism to store data over cloud storage in [13] a public auditability based technique is presented which provides a way to preserve security of the cloud data during the process of auditing. A secure auditing mechanism is presented in [14]. That uses a homomorphic authenticator to provide a proper and reliable framework for secure auditing of the in cloud storage. A survey over these techniques is presented in literature review section which provides a detailed overview over the techniques which used to provide privacy preserving in cloud storage.

Further this paper organizes as follows:

II Literature review, a brief review over the various techniques which used to provide security for the cloud data which stores at cloud server is presented in this section. III conclusion.

2. LITERATURE REVIEW

A brief review over the techniques which used to provide security in cloud storage is presented in this section. There are various techniques presented by the researchers, which provides an enhanced mechanism for secure storage in cloud.

Kadam Prasad, JadhavPoonam, KhupaseGauri, N. C. Thoutam [2] presents a system to transfer data from data owner to the user in cloud computing. In existing technique there is various type of issue like any unauthorized access provided to the user or data can be leaked during the process of transferring data. Thus in that technique, first user need to provide id and password to login to get authentication to access data then a request to access data is sent to the data owner. At data owners end data presents in encrypted form, that encryption provides security for the data if data get leaked during the process, a key to decrypt data is provided to the user. By the use of that key user can decrypt data and get access to that data. In that way integrity of the data maintained during the whole process. User does not get access to any other data except that authentication provided to the user because a key is required to access any data.

NiveditaSimbre, PriyaDeshpandey [5] presents a TPA and AES encryption based technique to provide security for the data over cloud. In this technique a file distribution mechanism is presented in that mechanism a SHA1 is used. When data distributed over cloud in that each block of the file contains its own hash code it provides a secure way of sharing of the data. Further encryption is also required, thus AES encryption is used to encrypt that data. In AES encryption, it is a symmetric key encryption technique which uses single for the encryption and decryption purpose. And TPA is used to provide auditing for that data. In this technique file verifies by comparing it hash values with the backup server's file hash value. This technique quite efficient to provides a secure way to access data over cloud.

Jian Liu, Kun Huang, Hong Rong [6] a regenerating code based public auditing technique is presented. In this technique, regenerating codes have lower repair bandwidth during fault tolerance. But it only supports public auditing and user need to be present during the whole process of auditing which is practically not possible. To reduce these short comings an

authenticator is designed which uses a proxy for the user in that user generate by using two public key and regenerated by the use of a partial key. In this technique a BLS authenticator is used which uses homographic properties and linear relations among the code blocks, in that way data owner is able to generate authenticator for the new method which quite efficient as compare to the existing technique.

Kai Hwang, Deyi Li [8] presents a data coloring and software water marking based technique is presented to enhance the security of the cloud. In which Data coloring and software watermarking is used to provide a trusted and secure environment to share data over cloud. In data coloring three parameters are used Ex (expected value), En (Entropy), He (Hyper entropy) to generate color. Ex is depends on data content on the other hand En and He Generate uncertainty and randomness these three parameters together generate a collection of cloud drop to generate "color" which is only known to the owner. And software watermarking is previously used to embed copyrights in digital documents but in this paper but in this paper watermarking is used in software modules to enhance the security of the cloud.

But in watermarking threats are there like crop variation, lossy compression and some other ways to manipulate images. Thus deformities can be also generated in software modules.

L. A. Dunning and R. Kresman [9] presented an anonymous ID assignment technique public cloud where multiple user access data simultaneously and parallel shared computing. In this technique an integer sharing technique is presented which used to provide security for data mining operation and perform iterations to assign AIDA for these operations. Most probably Newton's identities and Strum's theorem are used for data mining. It can also enhance to use for distributed data which can be enhances its scalability. But there is no proper mechanism for data sharing is presented.

In [19] author proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.in this research they have proposed identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats. A combination of PKI, LDAP and SSO can address most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh through federations, within which essential trust is maintained, with the technique provided by them a deep entity analysis can be able to perform and combine technique was able address various threads and issues related problem with the data and its integrity related to the data storage.

Slawomir Grzonkwoski, Peter M. Corcoran [11] presents authentication approach for home networking. A zero Knowledge proof based authentication approach is used to allow user to share their information with in a trusted environment like within an organization. It uses TCP/IP infrastructure to share information. In zero Knowledge proof protocol user need to prove the integrity of their data without revealing their data. In this way it does not require any knowledge about secret data to authenticate user. So in that way it uses user/password base service to authenticate user it enhance the security of the process in home network but in case of public network there are many attacks can be performed to get unauthorized access to that data.

Kan yang, XiaohuaJia [12] presents a dynamic secure auditing framework which to prevent privacy of the data from auditor. It uses cryptography techniques and bilinear paring to perform that task. Because it uses bilinear paring in place of masking technique thus it not require any organizer and provide batch auditing to multiple owners. It also provides a less communication cost and less computation cost frameworks to provide secure access to the user data. Dynamic auditing user can dynamically update their data. But in case of dynamic auditing there is case of replay attack and forge attack could be occurs, in replay attack data will not be updated at server thus server uses previous data rather than updated data. In forge attack server can be get enough knowledge about the data which can be able manipulate data or put forge tag in it.

Hemlatha, P Nirupama, V.Balaji [16] a decentralize access control technique is proposed which supports anonymous authentication. In this scheme authenticity of the series is verified and an access control mechanism is used which only allow only authorized user to access the data. And all the operation is perform in decentralized manner not like the other techniques which are centralized. In this technique there is no un-authenticated users can get access and in this way it can get the privacy preserving in cloud.

Madhumita S Patil, Santosh Kumar[17] a TPA based authentication technique is proposed in which authentication mechanism is achieved by the use of Third party auditor, it ensue that data can be accessed by the legitimate user in this mechanism at time of retrieval of the data a mechanism is required in which maintain the authentication otherwise this put huge overhead on user to maintain integrity of the data when more than one user access data simultaneously so third party auditor take care of that.

In [18] a redundant array based technique is presented to provide secure storage of the data. In that technique first data is segmented into different segments and distributed over the various storages. Relationship between these segments is private and secure from the other outside users. There is no information is provided to observer thus the observer cloud not able to reassemble the original file. Because each segment is very small and not contain enough information to provide details about the data. That way it provides confidentiality for the data and restrict outside user to get access to the data

Table 1.1: A comparison of the various techniques which used for the secure cloud storage in cloud computing

Technique	Advantages	Disadvantages
Redundant Array based technique [18]	Data is segmented into different subsets and then that segmented data in to different redundant array, in a distributed cloud storage. There is no TPA is required to store provide security for the data in cloud computing.	There is no monitoring for the process of storage is provide is provided

Dynamic Secure Auditing Framework [12]	Bilinear pairing and Cryptographic techniques are used to provide low computation cost and low communication cost	In dynamic auditing replay attack and forge attacks can be occurs
Zero knowledge proof protocol based technique [11]	In this user's personal information is not reveal to the others that preserves integrity of the data.	It not suitable to provide security in public network
Anonymous Id based technique [9]	provides an scalable data sharing mechanism by using anonymous ID for the operations	There is no suitable sharing mechanism is provided.
Data coloring and software watermarking technique[8]	A trusted data sharing mechanism in cloud computing is provided	Inherent defects of watermarking like crop variation, lossy compression are presents in this technique, which generates deformity in the data

3. CONCLUSION

A survey over the various techniques which used to provide security for the data resides over the cloud is presented in this paper. There are techniques like attribute based encryption, and some other symmetric and asymmetric key encryption techniques are presented by the researchers. There are some other techniques like homomorphic authenticator based auditing, privacy preserving techniques, attribute based encryption techniques are also presented that techniques used provide secure cloud storage and secure updation and auditing of the cloud data But these techniques suffer various performance issues. Thus a new enhanced technique to provide security for that data is proposed for future work.

There are various techniques which can be used for to provide a secure storage for cloud data. But these techniques suffers some defects like loss of data, losing integrity of the private file and or performed some attacks over cloud to get an unauthorized access for that data by any unauthorized user. Thus by the use of some encryption techniques like ABE (Attribute Based Encryption) or some other to maintain integrity of the data in cloud storage. Thus for future wok a hybrid technique which can be used to provide an enhanced technique, better performance and security to store data in cloud.

4. REFERENCES

[1] Tiantian LIU, Tongkai JI, Qiang YUE, Zhenchu TANG "G-Cloud: A Highly Reliable and Secure IaaS Platform" IEEE, 2015.

[2] KadamPrasad,JadhavPoonam,KhupaseGauri, N. C. Thoutam "Data Sharing Security and Privacy Preservation in Cloud Computing" IEEE, 2015.

[3] N. Shanmugakani, R. Chinna "An Explicit Integrity Verification Scheme for cloud Distributed systems" ICSO, IEEE, 2015.

[4] Mehmet SabirKiraz, Isa Sertkaya, OsmanbeyUzunkol "an Efficient Id based Message Recoverable Privacy Preserving Auditing scheme" PST, IEEE 2015.

[5] NiveditaSimbre, PriyaDeshpandey "Enhancing Distributed Data Storage security for cloud computing using TPA and AES algorithm" IEEE, 2015.

[6] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian "Privacy Preserving Public Auditing for Regenerating Code Based Cloud storage" IEEE, July 2015.

[7] Hong liu, Hua shengNing, QingXiong, Laurence T. yang "Shared Authority Based Privacy Preserving Authentication protocol in cloud" IEEE Transactions on Parallel and distributed system Vol. PP NO: 99, 2014.

[8] Kai Hwang, Deyi Li "Trusted cloud computing with secure resource and Data Coloring" IEEE 2010.

[9] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi Owner Data Sharing for Dynamic group in the cloud" IEEE Transactions on parallel and distributed system, 2012.

[11] Slawomir Grzonkwoski, Peter M. Corcoran "Sharing cloud service: User Authentication for social Enhancement of Home networking" IEEE Transaction on consumer electronics, Vol. 57, No. 3, August 2011.

[12] Kan yang, XiaohuaJia "An efficient and secure dynamic auditing protocol for data storage in cloud computing" IEEE transactions on parallel and distributed system, Vol. 24 No. 9, September 2013.

[13] Quin Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li "Enabling public auditability and data dynamics for storage data in cloud computing" IEEE Transactions on Parallel and distributed system, Vol. 22 No. 5, May 2011.

[14] C. Wang, Q Wang, K. Ran, N. Cao and W.Lou "Towards Secure and dependable storage service in cloud computing" IEEE Transactions on service computing Vol. 5, No. 2, 2012.

[15] https://en.wikipedia.org/wiki/Cloud_computing.

[16] Hemlatha, P Nirupama, V.Balaji "Anonymous Authentication for decentralized Access Control of cloud data" IJARCSMS, November 2014.

[17] Madhumita S Patil, Santosh Kumar" Study for Enhancement in privacy preserving authentication protocol using third party in cloud" IJEEM, Vol 3 Issue 1, 2013.

[18] MartinGiljeJaatun1,GansenZhao,AthanasiosVVasilakos,AsmundAhlmannNyre,StianAlapnesandYongTang"Thedesignofaredundantarrayofindependentnetstoragesforimprovedconfidentialityincloudcomputing"JournalofCloudComputing:Advances,SystemsandApplications2012.

[19] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009