Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Analytical Survey of Privacy Preserving Schemes in Cloud Computing

Saima Majeed[1], Er. Bandana Sharma[2]
[1]M Tech 4th semester, [2]Assistant Professor, Department of Computer Science
Haryana Engineering College Jagadhri, Kurushetra University, Haryana, India.

Abstract: ***Cloud computing has been considered as the next generation information technology architecture. It provides the potential to eradicate the requirements to set up the high cost computing infrastructure for IT –based services and solutions. It provides the flexible architecture which is accessible through Internet. This increases the capacity and capability of existing and new software. The cloud maintains and manages the data within various deployment models. Outsourcing the data gives a big relief for storage of data in local machines. However, there are multifaceted issues with respect to privacy and security of data in a cloud environment. This survey paper aims to study and compare various preserving schemes and methods to preserve security in a Cloud environment.***

Keywords: Platform as a Service (PaaS); Attribute based Encryption (ABE); Identity management (IDM); Infrastructure as a Service (IaaS); Software as a Service (SaaS); Trusted Third Party (TTP).

I. INTRODUCTION

Cloud computing is the concept of computing as a utility, where cloud customers can store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of computing resources which are highly configurable [6]. Its great flexibility and economic savings are encouraging both individuals and enterprises to outsource their local complex data managing system into the cloud, especially when the data produced by them that need to be stored and utilized is rapidly increasing. To protect data privacy and combat unnecessary accesses in cloud, it may have to be encrypted before outsourcing to commercial public cloud by service providers [7] this, however, outdates the traditional data utilization service which is based on plaintext keyword search.

II. CLOUD TAXONOMY

A. *Characteristics and Benefits*

Cloud computing can be defined based on the services provided and deployment models. According to the various types of services offered, cloud computing consists of three layers. Platform as a Service (*PaaS)* layer provides environment for operating systems, applications, virtual machines, services, frameworks, transactions, and control structures. The client can deploy its applications on cloud infrastructure that were programmed using languages supported by PaaS service provider. Infrastructure as a Service (*IaaS)* is the lowest layer which provides basic infrastructure support as well as service. Software as a Service *(SaaS)* is the topmost layer which offers the service on demand for a complete application [11, 12].

Regardless of the above mentioned service models, cloud services can be expanded in four ways depending upon the requirements of customer:

1) *Public Cloud:* A cloud infrastructure which is managed by third party provides services to many customers; various enterprises can work on the framework provided, at the same time [13]. Users can dynamically plan resources through the internet from an off-site service provider. Wastage of resources is analyzed as the users pay for whatever they use.
2) *Private Cloud:* Cloud framework, managed either by the organization itself or third party service provider is made available only to a specific customer [13].This uses the approach of virtualization of machines and is a proprietary network.
3) *Community Cloud:* It is managed by third party server and shared by several organizations.
4) *Hybrid Cloud:* It is the combination of two or more cloud deployment models, linked in a way such that transferring of data will take place without affecting one another. Each model retains their unique identities, but works together as a unit.

B. *Architecture of Cloud Model*

Considering a cloud data hosting service involving three different entities, data owner, data user, and cloud server, as illustrated in

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Figure 1.

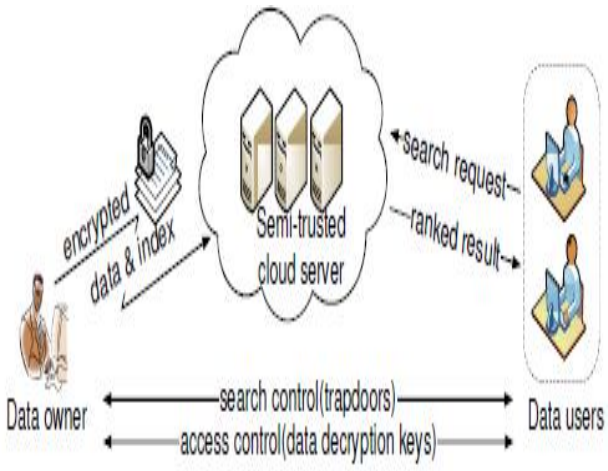

Figure1. Architecture of the search over encrypted cloud data [4]

To improve document retrieval accuracy, search result should be arranged by cloud server as per some ranking basis. Finally, the access control mechanism is used to manage decryption proficiency given to users [4].

III. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing is now termed as the fifth basic service after gas, water, electricity, and telephony [9] .There are various cloud computing service models, viz Infrastructure (e.g., Amazon's EC2, AmazonS3, IBM Blue cloud), Platform (e.g., Yahoo Pig, Google App Engine), and Software (e.g., saleforce.com, Gmail, Microsoft online) as a service. Users neither need to invest in their own software/hardware systems nor to hire any IT professionals. One of the major concerns for storing the data in a cloud is security and privacy. Therefore various techniques and security algorithms have been designed to overcome this problem. These include encryption, stringent access, limited service access and data backup and recovery to make retrieval of data easy. In order to secure the confidentiality and privacy of data from a cloud service provider, one of the encryption techniques used is illustrated in Figure 2 [5].

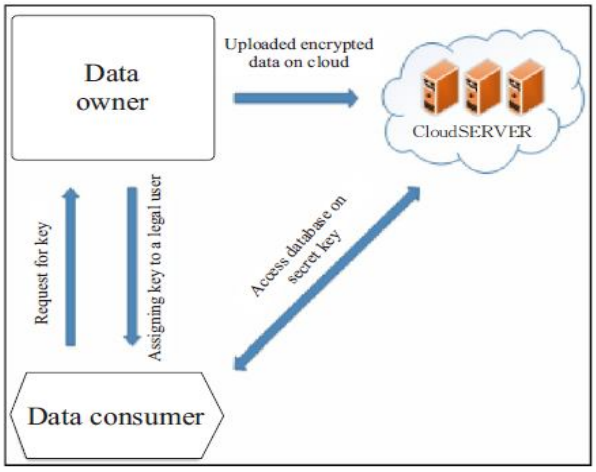

Figure2. Secure data Access in Cloud [5]

Attribute-Based Encryption (ABE) is one of the recently public key cryptographic techniques that works in an onto-many fashion and is also called fuzzy encryption. Public key encryption methods store the data which has to be encrypting on third party servers, and the same time distribute decryption keys to authorized users. However, there are many limitations of public key encryption method. First, it is quite difficult to manage the distribution of secret keys to authorized users. This technique provides less flexibility as well as scalability. Data owners must be online whenever encrypting or re-encrypting data, or during the distribution of

the secret keys. ABE lessens the above limitations by reducing the communication overhead of the internet and on the same time increases scalability, flexibility, and fine-grained access control for large scale systems [14].
Ideal ABE scheme [10] is similar to public key based mechanism where a secret key is dependent on attribute count.
Following definitions provide an introduction overview of accountability, confidentiality, collisionresistance and secure access control.

A. Data Confidentiality
The data is encrypted by the data owner before uploading it to the cloud. Unauthorized users cannot access the data.

B. Fine-Grained Access Control
It provides the safe ease of access to the resources. During accessibility, user's access rights are not the same within a group.

C. Scalability
The performance of the system is not affected if the number of authorized users increases.

D. User Accountability
All the authorized users should make sure not to share their private keys with illegal users.

E. User Revocation
If any user wants to quit the system, the system revokes the access rights directly, and the user will no longer have right to access to any stored data.

F. Collision Resistance
It is not possible for users to decipher encrypted data by combining their attributes, since each attribute is related to a random number or polynomial.

IV. LITERATURE SURVEY

Ranchal et al. (2010) discussed that Identity management (IDM) which is considered to be one of the important components in cloud privacy and security, helps to ease some of the problems associated with cloud computing. In identifying entities to SPs, the available solutions use trusted third party (TTP). This is an approach for IDM that has the ability to use identity data on entrusted hosts and is independent of TTP. The approach uses predicate multi-party computing for negotiating a use of a cloud service and uses predicates over encrypted data. It uses active bundle which is a middleware agent that has a set of protection mechanism and also includes the privacy policies, PII data, virtual machine that enforces the policies. To authenticate a user to cloud services, an active bundle interacts on behalf of a user with it using privacy policies of a user [1].
D. Srinivas (2011) makes use of the homomorphism non- linear authenticator and random masking to assure that the Third Party Auditor (TPA) would not find out any information about the data content which has to be stored on the cloud server during the auditing process so that it not only removes the burden of cloud user from the tiresome and possibly expensive auditing task, but also relieves the users' fear of their outsourced data leakage [2].
Wang et al. (2012) discussed that the cloud enables the users to store their data on pay per basis without the burden of local hardware and software management. Though the benefits are quite visible, however such service also back downs the user's physical possession of their outsourced data, which essentially poses new security threats towards the correctness of the data in cloud. A flexible distributed storage auditing mechanism with distributed erasure-coded data and homomorphic token is taken into account to overcome this problem. It allows users to audit the cloud storage having lightweight communication and computation cost as well. Auditing result ensures both strong cloud storage correctness as well as simultaneously helps to detect data error. Considering the fact that cloud data is dynamic in nature, it provides the secure and efficient operations on outsourced data which are modifications of block, append and deletion. This scheme is highly efficient and elastic against all failures as well as malicious data modification attacks [3].
Cao et al (2014) defines as well as solves the problem which is a challenging issue of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and creates a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, it choose the efficient principle of "coordinate matching", i.e., as many matches as possible, which captures the similarity between data document and search query , and further use "inner product similarity" to quantitatively define such principle for measurement of similarity. It includes a basic MRSE scheme that uses inner product computation, and then considerably improves it so as to improve the different privacy requirements in two levels of threat models. The proposed schemes introduce low overhead on computation and communication through careful analysis investigating

Volume 5 Issue IV, April 2017
ISSN: 2321-9653

privacy and efficiency guarantees of proposed schemes as well as experiments on the real-world dataset [4].

Shabir et al. (2016) discussed that the cloud computing has become an important computing model in the IT industry. In this emerging model, computing resources which include software, hardware, networking, and storage can be accessed on a pay-per-use basis anywhere in world. However, it's still a challenging issue to store the sensitive data on un-trusted servers in a cloud. In order to ensure the confidentiality and proper access control of sensitive data, various classical encryption techniques have been implemented from time to time to lessen the security breach in a cloud. However, because of lack of flexibility, scalability and fine-grained access control, these access control schemes are very less feasible in cloud computing. To overcome these limitations, Attribute-Based Encryption (ABE) techniques are used in the cloud. This paper includes all ABE schemes as the well as the key criteria used in these schemes [5].

Table I Comparative analysis of some of the existing security schemes

Author	Details of Existing Security Schemes			
	Approach	*Year*	*References*	*Findings*
Rachal et al	Identity Management(IDM) independent of trusted third party(TTP) using active bundle.	2010	1	1. Ability to authenticate without disclosing unencrypted data, which can be achieved by using predicate over encrypted data. 2. Protection of identity data from untrusted hosts. 3. No need for TTPs

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Author	Details of Existing Security Schemes			
	Approach	*Year*	*References*	*Findings*
D. Srinivas	RSAbased Homomorphic non linear authenticator and random masking.	2011	2	1. This approach assures that the Third Party Auditor (TPA) would not find out any information about the data content which has to be stored on the cloud server during the auditing process. 2. This scheme is highly efficient and secure.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Author	Details of Existing Security Schemes			
	Approach	*Year*	*References*	*Findings*
Cong Wang et al	Distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data.	2012	3	1. It provides the storage correctness i.e., it ensures the users that the data is securely stored and kept intact in cloud. 2. It brings in efficient and dynamic operations on outsourced data, which includes modification of block, deletion, and append. 2. Highly efficient and resilient against all failures as well as malicious attacks.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Author	Details of Existing Security Schemes			
	Approach	*Year*	*References*	*Findings*
Ning Cao et al	Multi-keyword ranked search over encrypted cloud data (MRSE) scheme.	2014	4	1. It provides the set of privacy requirements for securing the cloud by solving the problem of multi-keyword ranked search. 2. It brings in concept of low overhead on both computation and communicatio n.
Shabir et al	Attribute Based Encryption (ABE) schemes.	2016	5	1. It reduces the computation overhead as well as the cipher text size. 2. It offers fine-grained access control. 3. Flexibility and scalability in cloud computing.

V. CONCLUSION

In this paper, we have studied the concept of cloud computing and the various privacy preserving schemes in cloud. One of such scheme is Identity Management (IDM) independent of trusted third party (TTP) using active bundle. It provides the ability to authenticate without disclosing unencrypted data, which can be achieved by using predicate over encrypted data and protection of identity data from entrusted hosts. RSAbased Homomorphic non linear authenticator, this scheme assures that the Third Party Auditor (TPA) would not find out any information about the data content which has to be stored on the cloud server during the auditing process, also secure and efficient scheme. Distributed storage integrity auditing mechanism, this scheme guarantees strong cloud storage correctness and achieves the fast data error localization and highly efficient and resilient against Byzantine failure, malicious data. Homomorphic linear authenticator, this scheme eliminates the burden of cloud user from the tedious and possibly

expensive auditing and also enables multi-user setting. Attribute Based Encryption (ABE) scheme, it gives users access to stronger encryption, allows key strength distribution and offers fine-grained access control, flexibility, and scalability in cloud computing.

REFERENCES

[1] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, Mark Linderman,"Protection of Identity Information in Cloud Computing without Trusted Third Party", 29th IEEE International Symposium on Reliable Distributed System,2010.

[2] D. Srinivas, "Privacy-Preserving Public Auditing In Cloud Storage Security," D.Srinivas (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2691-2693.

[3] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Cloud Computing Date of Publication: April-June 2012 Volume: 5 , Issue: 2.

[4] Ning Cao, Cong Wang, Ming Li, Kui Ren,Wenjing Lou, "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data, " IEEE Transactions on Parallel and Distributed Cloud Computing Systems,Volume:25,Issue:1,Issue Date:Jan.2014.

[5] Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood_, and AtaUllah Ghafoor,' "Analysis of Classical Encryption Techniques in Cloud Computing," TSINGHUA SCIENCE ANDTECHNOLOGY ISSN 1007-0214 09/10 pp102-113 Volume 21, Number 1, February 2016.

[6] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009.

[7] S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS. Springer, Heidelberg.

[8] S. Zerr, E. Demidova, D. Olmedilla, W. Nejdl, M. Winslett, and S. Mitra, "Zerber: r-confidential indexing for distributed documents," in Proc. Of EDBT, 2008, pp. 287–298.

[9] Z.Wan, J. E. Liu, and R. H. Deng, A hierarchical attribute based solution for flexible and scalable access control,IEEE Transactions on Information Forensics and Security,vol. 7, no. 2, pp. 743–754, 2012.

[10] C. C. Lee, P. Chung, and M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud enviornments,International Journal of Network Security",vol.15, no. 4,pp. 231-240,2013.

[11] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing", Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[12] B.P. Rimal, Choi Eunmi, I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Intl. Joint Conference on INC, IMS and IDC, 2009, pp. 44-51, Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218.

[13] R. L. Grossman, "The Case for Cloud Computing", IT Professional, vol. 11(2), pp. 23-27, Mar-April, 2009, ISSN: 1520-9202, INSPEC Accession Number, 10518970, DOI: 10.1109/MITP.2009.40.

[14] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Transactions on Parallel and Distributed Systems, vol. 24,no. 1, pp. 131–143, 2013.