CLOUD COMPUTING AND METHODS FOR PRIVACY PRESERVATION: A SURVEY

Mr. R. Nallakumar,Dr. N. Sengottaiyan, M.MohamedArif

***ABSTRACT:*Cloud computing is a emerging trend in the technology side. With the development of networking and internet, the ability of technology to enable mankind to get access to any nook and corner of the world has seen greater heights. Clouds can store large amount of data without consuming ones real system space. But on the other side, the data stored in cloud must be preserved. There are many privacy preserving methods in the existing side to prevent the data in cloud. TPA's are also one such. This survey discusses the concepts of cloud and the methods to preserve the privacy of the data on cloud storage.**

***KEYWORDS:* cloud security, privacy, utility computing, public auditing, third party agents, services.**

I. INTRODUCTION

Science and technology is on the developing verge. Technology has bought many changes. Earlier it was only IT 's competing for space with science. But now-a-days everybody are twined with technology. As day passes, people want more and more from technology. Many wonders are being made through science. One such is Cloud Computing. To satisfy the thirst of IT's and people, Cloud Computing is on the new dimension. The terms outsourcing and elasticity are quite common and important in tech fields. These two terms saw the rise of this new dimension of Utility Computing.

Manuscript received, Nov 2014
***R.Nallakumar,** Assistant Professor, Dept. of CSE, Anna University Regional Centre, Coimbatore-47.*

***Dr. N.Sengottaiyan,** Professor, Dept of CSE, Indira Institute of Engineering and Technology,Chennai.*

***M.Mohammed Arif,**PG Scholar, Dept of CSE, Anna University Regional Centre, Coimbatore-47.*

Cloud Computing is a sort of utility computing serving to the needs and demands of all types of users perfectly. In the present scenario, large IT firms are outsourcing huge amount of their products and services. At such times, the resource elasticity of that firm will show up its status. These Two statures are completely handled by Cloud Computing. But in the recent times, there are confusions and talks on clouds. In a statement Oracle CEO rightly expressed his frustration," ….. the interesting thing about Cloud computing is the we've redefined cloud computing to include everything that we already do… I don't understand what we would differently do in the light of cloud computing other than changing the wordings of some of our ads."

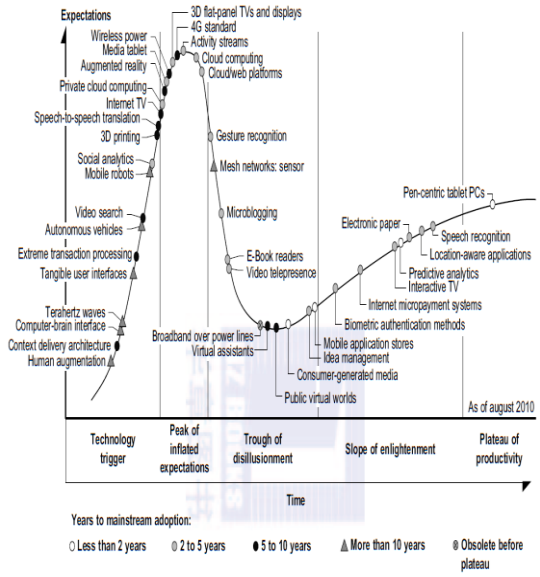

Fig 1[1]: Hype Cycle for Emerging technologies Since 2010

Cloud computing can be thus rightly defined as both applications that delivers services over the internet at our hands and also the hardware and softwares installed at the data centers to deliver the services. The concept of cloud computing is never bound between a consumer and provider. It involves many roles like auditor, carrier, broker,

ISSN: 2278 – 1323

provider and consumer. But what these services mean? Services provided by cloud are just a click , easy to use and pay to use. Literally they are the Iaas, Paas, and Saas. These services are made available to the users through the carriers and providers. Cloud also provides storage. Cloud storage is increasingly popular because of its dimensionality. One can store volumes of data without having to use one's physical system space. Thus the concept of *virtualization* is made possible. In the present day, the amount of data in any cloud is difficult to measure. But the problem is that when highly confidential data is being stored in a private space , security is the commercial aspect. The data that is stored in cloud is made secure through many methods. The remaining sections of this paper discusses some real world basics of cloud and the methods for security of data in cloud.
Section II discusses the roles in cloud. Section III discusses the various methods for preserving privacy in cloud. Section IV concludes the survey with some future works.

II. THE CLOUD MODEL

Cloud computing is a shared pool of resources that is provisioned by some provider. The only demand for using cloud is the availability of internet access.

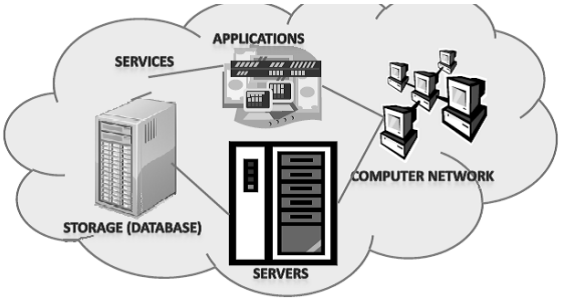

Fig 2: A Cloud Environment

A model or reference architecture has been devised by NIST (National Institute of Standards and Technology). According to it, the availability of cloud services does not only depend on the provider but also on the other roles in the scenario.

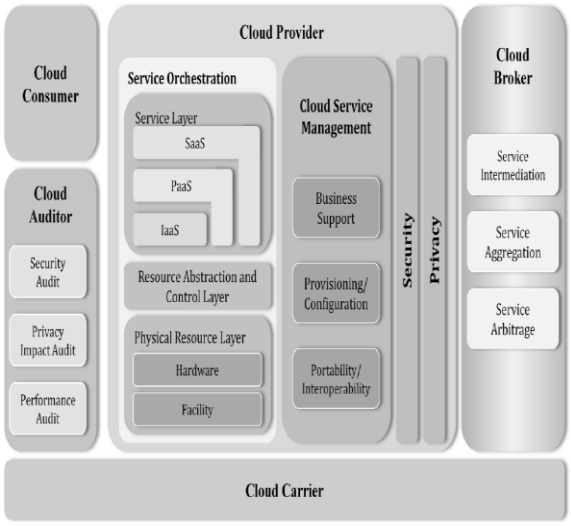

Fig 3[1]: The Conceptual Reference model proposed by NIST

The cloud provider can be a person or a private organization or a government organization. There are many providers like Google, Amazon, Microsoft, etc.. Providers ensure that proper arrangements are made to deliver the services. Cloud consumers must make Service Level Agreements with the providers to avail the services. The rely on brokers and carriers for the completely availing the services. The integrity of these services are duly checked by the auditors. Some of the services are:
Iaas: Storage, backup, recovery, platform hosting, computing, services management.
Paas: Development, Testing, Database, Business Intelligence, Application development.
Saas: Document management, E-mails, Content management, financials, office suite, sales, ERP, Human resources.
The cloud is generally deployed in four forms: public cloud, private cloud, community cloud and hybrid cloud. As the name tells, Public clouds are accessible to anyone. These are generally owned by a large organization that servers the commercial needs of the people. Examples are Amazon EC2, Google App Engine, Microsoft Azure. Private clouds are those that are owned by a separate organization for their purpose but not for the general. Access to these clouds require the prior permission of the authority. Examples are Eucalyptus, Ubuntu Enterprise cloud, Microsoft ECI data center. Community clouds are those owned by a community for shared concerns. Hybrid cloud is a mixture of all the above. As discussed so far, there are many components and services in the world of Cloud computing. But how are they maintained? Cloud is maintained through the Data Centers. A data centre will have numerous hardware systems and their maintenance personnels in a sophisticated

ISSN: 2278 – 1323

environment. It is here the cloud data gets stored and maintained.

III. CLOUD DATA STORAGE

Cloud storage is a boon to people who wants to maintain large amount of data. Cloud provides virtual data storage. The storage functionality is implemented in any shared block device. The shared block device can be accessed over the network. There are issues in this shared block device method. The main one is data security and privacy. It would be difficult for anyone to store confidential data in someone's storage area. The next issue is data integrity. The stored data must remain the same as stored initially. To solve these issues, an authentication mechanism is necessary for anyone to access cloud. Many methods are available to preserve the privacy and integrity of the data in cloud.

PRIVACY PRESERVING METHODS:

A. DATA PARTIONING TECHNIQUE
B. PccP MODEL FOR CLOUD
C. ORUTA
D. SECURITY MEDIATOR
E. PRIVACY PRESERVING ACCESS CONTROL

A. DATA PARTIONING TECHNIQUE:

The dynamic processing of data from the storage device upon the end user's request takes huge time. This drawback is overcome in the data partioning technique. The implementation of this system has the following stages: end-user, cloud storage server, access data from cloud storage service, cloud exchange, RSA encryption and decryption, MD5 Message Digest Algorithm, Partioning algorithm. In this technique, the end user first requests for data access. The remote integrity of the end user is checked. AES algorithm is used to store the End User Client data. RSA algorithm is used to store the details of the storage server. The Data integrity is checked using the MD5 message digest algorithm. The data partioning algorithm is as follows:

Algorithm for Data Partioning[]:

1. The input file is loaded.
2. First two letters are retrieved and checked for folder.
3. If folder is not present, create one.
4. Encrypt the partition file using the public key
5. Decrypt the original file using the private key without having to access the data center.

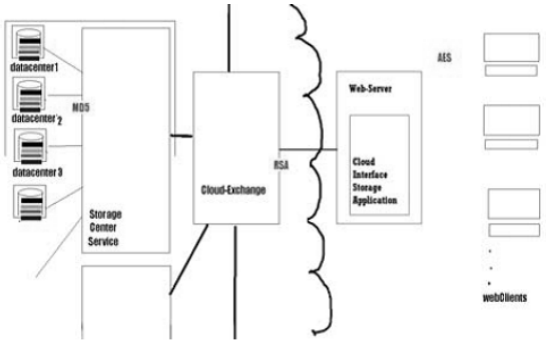

Fig 4[] : Cloud data partioning

This data partioning plays an important part as storing and retrieving large file is difficult in cloud. Also the retrieval is highly secure and integrity is greatly preserved.

B. PccP MODEL FOR CLOUD

The PccP model of cloud architecture is another model for preserving cloud privacy. This is a layered model where the Consumer layer forms the basement layer. Users submit their request through this layer. The requests submitted by the users are translated by the Network Interface or the Address Mapping Layer. This layer translates the IP address of the user request thus preserving the privacy according to the access request file. An Unique User Cloud Identity is generated and allows the user to specify the access control and the amount of Data Transparency. A Boolean function named Transparency Purpose in Cloud is carried out to specify the Personal Data Attribute of the data transparency. Thus this mechanism checks for both access control and user identification.

C. ORUTA

The data in a cloud is generally publicly shared. Third party auditors generally audit the shared data in cloud. In this method, public auditing of the shared data is possible while still the identity of the signer of the shared data kept hidden from TPA. The design objectives of this system are public auditing, identity preserving, unforgetability, correctness. The concepts of Homomorphic Authenticable Ring Structures are exploited. With these ring structures, the signatures of the original user and the group user would be mixed, thus making it difficult to identify the signer for TPA. The construction of Oruta includes four algorithms: **KeyGen, SigGen, ProofGen, ProofVerify**.

ISSN: 2278 – 1323

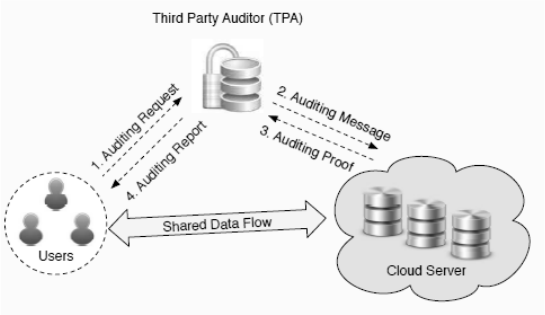

Fig 5[3]: Oruta Model

D. SECURITY MEDIATOR

Because of the security concerns and the concerns on the data integrity , Provable Data Possession must be verified before finalizing with the outsourced data. But this PDP exposes the identity of the owner to untrusted verifiers. To overcome this problem , Security Mediator has been designed and modeled. The design goals of this system are:

- Public verifiability
- Verification efficiency
- Unforgetability
- Anonymity
- Data privacy
- Signing efficiency

This system uses the concept of Blind Signatures. They are a form of message sending where the owner and signer are different. The owner blinds the message and sends it to the signer to sign. The signer signs the message and sends it back. The owner outputs the original sign based on the result of the signer and the blinding factor she has chosen.

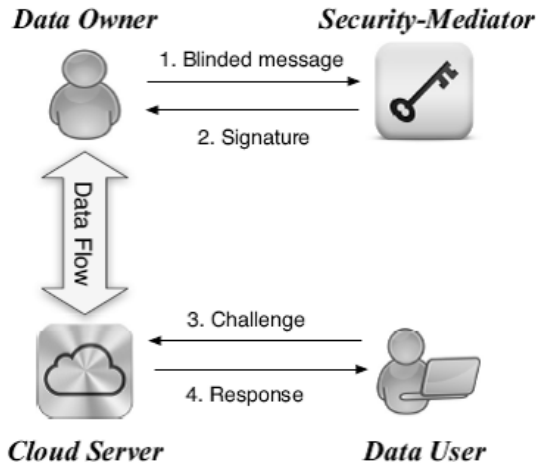

Fig 6[4]: security mediator model.

In order to reduce the communication overhead, the owner first integrates all the blocks of data into single block.

E. PRIVACY PRESERVING ACCESS CONTROL:

Miao Zhou et al [15] in his work considered the privacy of the data through the access rights given for each user. The data privacy is sought using a two tier encryption architecture model. The base phase and the surface phase. In the base phase, the owner performs the local encryption on the outsourcing data. In the surface phase, the server performs Server re-encryption Mechanism on the data to be outsourced. This SRM mechanism preserves the full access control of the user. It does no compromise on the user's privilege and does not disclose the owner to cloud provider.

Some acts that fail to protect the privacy of information in cloud:

1. ECPA- Electronic Communications Privacy Act [9]

2. UPA- USA Patriot Act [7]

3. HIPAA- Health Insurance Portability And Accountability Act [10]

4. FCRA- Fair Credit Reporting Act [11]

5. VPPA- Video Privacy Protection Act [12]

6. GLBA- Gramm Leach Bliley Act [13]

7. CCPA- Cable Communications Policy Act [14]

IV. CONCLUSION

Cloud computing is a developing technology. It has brought a new dimension in the tech trend. Its ability to store volumes of data has gained greater popularity. On the other side, the security issues are also increasing. This paper has discussed some of the methods for preserving privacy and integrity in cloud. Ad day passes, cloud data outsourcing is in the growing trend. Similarly outsourcing threats are also in the rise. Also powerful security mechanisms parallel to traditional encryption is being developed.

The future of this paper would be to extend methods like Oruta and privacy preserving for outsourced data.

REFERENCES:

[1]Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, NIST REFERENCE ARCHITECTURE, Special Publication 500-292.

ISSN: 2278 – 1323

[2] T. JothiNeela and N. Saravanan,Privacy Preserving Approaches in Cloud: a Survey, Indian Journal of Science and Technology.

[3]BoyangWang ,Baochun Li and Hui Li, Oruta: Privacy-Preserving Public Auditing for0 Shared Data in the Cloud, 2012 IEEE Fifth International Conference on Cloud Computing

[4] Boyang Wang , Sherman S.M. Chow , Ming Li , and Hui Li, Storing Shared Data on the Cloud via Security-Mediator, 2013 IEEE 33rd International Conference on Distributed Computing Systems.

[5]Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica, and MateiZaharia, A View Of Cloud Computing, ACM.

[6]Boyang Wang†, Baochun Li, Hui Li and Fenghua Li, Certificateless Public Auditing for Data Integrity in the Cloud, 2013 IEEE Conference on Communications and Network Security (CNS).

[7]M. McCarthy, "USA Patriot Act," Harv. J. on Legis., vol. 39, p. 435, 2002.

[8] R. Gellman, "Privacy in the Clouds:Risks to Privacy and Confidentiality from Cloud Computing," www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf, 2009.

[9] R. Burnside, "Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies, The," Rutgers Computer & Tech. LJ, vol. 13, p. 451, 1987.

[10] S. Dwyer III, A. Weaver, and K. Hughes, "Health Insurance Portability and Accountability Act," Security Issues in the Digital Medical Enterprise.

[11] F. Act, "Fair Credit Reporting Act," Flood Disaster Protection Act and Financial Institute.

[12] EPIC.org, "Video Privacy Protection Act," http://epic.org/privacy/vppa/.

[13] A. Akhigbe and A. Whyte, "The Gramm-Leach-Bliley Act of 1999: Risk implications for the financial services industry," Journal of Financial Research, vol. 27, no. 3, pp. 435–446, 2004.

[14] P. Parsons and R. Frieden, The cable and satellite television industries.

[15] Zhou M, Mu Y et al. (2011). Privacy-Preserved Access Control 3. for Cloud Computing, International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 83–90.

Mr. R. Nallakumar received the BachelorDegree in Computer Science andEngineering in 2009. He received the Masterdegree in Computer Science and Engineeringin 2011. He also completed Master ofBusiness Administration and currently he ispursuing his Ph.D. He is working as an Assistant professor at Anna University Regional Centre,Coimbatore, Tamilnadu, India. His area of interest is CloudComputing.

Dr. N. Sengottaiyan received the BachelorDegree in Electronics and CommunicationEngineering in 1986. He received the MasterDegree in Computer Science andEngineering in 2004. He has received hisPh.D in 2011. He is currently pursuingP.D.F from California South University,California,U.S.A. He is working as a Principal at IndiraInstitute of Engineering and Technology Thiruvallur,Chennai, Tamilnadu, India. His area of interest are CloudComputing and Wireless Sensor Networks.

M.MohamedArif received the BachelorDegree in Computer Science andEngineering in 2013.he is currently pursuing Master Degree in Software Engineering at Anna University Regional Centre,Coimbatore, Tamilnadu, India. His area of interest is CloudComputing.

ISSN: 2278 – 1323