ISSN:0975-9646

Privacy Preserving Issues and their Solutions in Cloud Computing: A Survey

Pooja HP [1],

MTech(CSE), BMSCE, Bangalore, India.

Nagarathna N [2]

Prof. Dept. of CSE, BMSCE, Bangalore,India.

Abstract: - Cloud computing is a type of computing wherein instead of having local servers or personal devices to handle applications it trusts on sharing computing resources. The aim of the Cloud computing is to provide inexpensive and scalable on-demand computing service. Data can be accessed from any place without retaining local copy of data in cloud storage. But the major problem is Data security. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a Third Party Auditor (TPA) to check the integrity of outsourced data. Lot of investigation has been made to identify the issues with these cloud service providers and cloud security. This paper explores security issues and various problems faced by cloud users and service providers. Also, various security threats and reinforcing approaches utilized for resolving the privacy issues in cloud resources are analyzed.

Keywords: Cloud storage, Cloud computing models, Third Party Auditor (TPA), Security issues, Privacy Preserving Schemes.

I. Introduction

Cloud computing is an important technology that comes first among top ten important technologies [1]. Cloud computing is a method in which memory, computing power, infrastructure can be delivered as a service. A Cloud computing is a set of network enabled services with guaranteed QoS, inexpensive computing infrastructures on demand with an easy and simple access [2] [3]. Cloud security is an evolving sub-domain of computer security, network and information security. Security in cloud can be implemented remotely by client.

The objectives of the service provider are:

- Confidentiality for securing the data access and transfer
- Ensuring integrity in cloud information.
- Auditability for checking whether the security aspect of applications has been tampered or not [4].

A. Cloud Service Models

The Cloud computing service models are divided into three categories as shown in Fig.1 Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [5] [6].

1) *SaaS:* It makes use of Cloud computing infrastructure for the purpose of delivering one application to many users. It is also called as on demand service. As long as the computer has internet connection, SaaS is an application that can be accessed from anywhere in the world. This cloud hosted application is accessed without any additional hardware and software. It also provides security feature like SSL Encryption which is a cryptographic protocol. Examples: - Yahoo Mail, Hotmail, G-Mail.
2) *IaaS:* It is virtual delivery of computing resources in the form of storage services, hardware and networking. Optionally, it includes distribution of operating systems and virtualization technology to manage the resources. Companies rent these resources as needed, instead of buying and then installing the required resources in their own data center. Examples: - Google Apps, Microsoft Office.
3) *PaaS:* Cloud Providers deliver a computing platform and solution stack typically including operating system, Database, Web Server, and programming language execution environment. Examples: - Windows Azure, AWS Elastic Beanstalk, Force.com, Apache Stratos, Google App Engine.

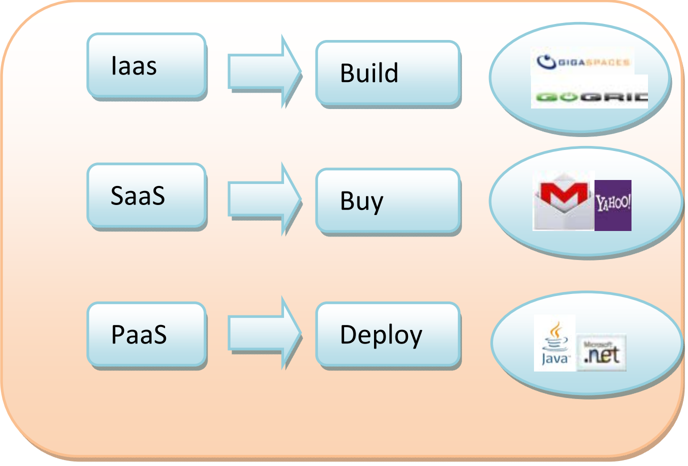

Fig.1 Cloud computing models

These three models are called as delivery models which provide basic functions of cloud management system.

B. Cloud Computing Components

The functions of cloud management system are broadly partitioned into five layers [7] [8]:

1) *User Layer:* Functions like Administration, End-user, and Partner are managed by this layer.
2) *Access Layer:* Functions like Inter-Cloud peering, federation function and API termination are managed by this layer.

3) *Network Layer (Resource Layer):* The physical and virtual resources managed by this layer.
4) *Service Layer:* Functions like service orchestration, service automated arrangement, cloud operational function and Cloud service categories such as SaaS, IaaS and PaaS are managed by this layer.
5) *Cross Layer:* Security, Privacy and Management functions are specified in this layer.

C. Cloud Storage

Cloud storage is an online file storage center. It is an important service model in cloud computing, which allows owners to share data from their local computing system to cloud. These cloud storage providers are responsible for keeping the data available and attainable, and the physical environment protected and running. The Cloud storage provider allows uploading files to the internet safely. There are various providers of cloud storage, for example Apple iCloud, Drop box, Google Drive.

Cloud computing comes with numerous possibilities and challenges simultaneously. Security is one of the main challenges that hinder the growth of cloud computing. The security challenges for cloud computing are somewhat dynamic and broad.

II. CLOUD SECURITY ISSUES

Security in cloud is a challenge where confidentiality, integrity and authentication are the crucial areas. Due to lack of knowledge about responsibility among service providers and users, there exist many conflicts. Data location is a vital role in Cloud computing security. Location transparency is one of the prominent flexibilities for cloud computing, this is a security threat at the same time – without knowing the specific location of data storehouse, the provision of data protection act for some region might be severely affected and violated. Users' personal data security is thus a crucial concern in a cloud computing environment. Cloud computing has many advantages such as: we can easily upload and download the data stored in the cloud. We can access the data from anywhere, any time on demand. Cost is low and it is done on a pay per usage basis. Hardware and software resources are easily available without location independent. But the main disadvantage of Cloud computing is security.

In Cloud computing, security issues have two levels:

- *Provider level:* In this level, it is important to make sure that the server is well secured from all the external attacks it would come across.
- *User level:* Although the service provider gives a good security layer, it is important for the users to make sure that there is no stealing of data or tampering or loss of data.

The Cloud Security Issues are broadly classified as:

A. Data Issues
B. Privacy and legal issues
C. Malicious application

A. Data Issues

In cloud computing environment, securing sensitive data is a critical issue.

1) *Integrity:* Whenever data is stored on cloud, there are chances of data being accessed by anyone from any place. Sometimes, many cloud users and providers could access and modify the data simultaneously. Hence data integrity is required to protect user's private and sensitive information.
2) *Availability:* Whenever the users access data, it should be available to them in expected/correct format.
3) *Data Theft:* This is a major issue in a cloud computing. Some cloud service providers obtain server from other service providers instead of providing their own server, as it is flexible and cost effective for cloud providers. So there are more chances of data being stolen from the external server.
4) *Data Loss:* Loss of data is another common problem in cloud computing. If cloud user winds up his services due to any problem, there will be huge loss of data. Moreover, data can be lost or damaged or corrupted due to natural disaster or fire which would make data inaccessible to users.
5) *Data location:* This is another issue that has to been taken care in cloud computing environment. Knowledge about physical location of data- Where data is stored? How data is stored? - is important. Cloud service providers do not specify where user's data is stored. Hence, data location should be transparent to users and customers.
6) *Viruses and Worms:* They are malicious codes that corrupt files on local file system and decreases the performance of application and hardware.
7) *Spoofing:* To gain access on a network, an attacker impersonates the users as the originator of the message.
8) *Replay:* It is a type of attack where an attacker reads/gain the information sent from originator and then resends it to receiver.
9) *Man-in-the-Middle Attack:* Here, an attacker monitors the communication between two parties and modifies the messages.
10) *Eavesdropping:* An attacker obtains access in the data path, tries to monitor and read the messages.

These are major data issues that need to be handled in an effective manner. Privacy is another major issue in cloud computing.

B. Privacy Issues

In cloud computing, a service provider should make sure that user's and customer's information is secured efficiently. Also, the cloud service provider should know who is maintaining the server and who is accessing the data so as to ensure that only authorized users are allowed to access data and customer's information is protected. This ensures only authenticated and authorized users accessing data [9]. As users are made to give their personal information without knowledge of where it is stored or how it is stored, there are chances that the cloud vendors would reveal sensitive or personal information.

Hence it is important that cloud vendors or cloud service providers should ensure that users' privacy is maintained.

Apart from data issue and privacy issue, there are chances of data/application being infected which is another issue in security [10].

C. Malicious/Infected Application

Sometimes malicious users upload infected application/data to cloud which would affect other users and customers. To monitor and maintain server, Cloud service providers should have complete access to the server. Hence, this prevents any user from uploading malicious or infected application on to the cloud.

A cloud is better only when service provider provides good security to the users and customers. In order to overcome these security issues, efficient encryption algorithms should be adopted. Some methods/schemes are specified below.

III. Privacy Preserving And Public Auditing Schemes

Different approaches have been put forward to implement the issue of privacy preserving. This paper studies some of the approaches and provides a brief review. It is important to ensure that privacy is preserved in all the situations. So, the work takes us in both tracks: preserving the privacy of the data as well as preserving the privacy while we prefer some third party auditing to assure the data correctness.

A. Privacy Preserving Schemes

The main role of the service providers is to maintain privacy of the users where their confidential information is stored in the cloud. Due to insufficient user control, information disclosure, uncontrolled data proliferation, unauthorized second storage and dynamic provision there exists few issues that could lead cloud service providers to attain privacy. In paper [11], various security threats and issues that affect the privacy preservation of the data users are analysed. Also, the methodologies used to solve the security threats are analysed. Different cryptographic mechanisms that are used to resolve the security threats are specified.

1) *Public Key based Homomorphic Linear Authentication (HLA):* This scheme presents Privacy Preserving and Public Auditing for Data in Cloud Storage. Data Security is a major issue in Cloud computing that needs to be considered. The users store their data in file server without keeping local copy in the cloud where they cannot trust the clients and unreliable server. Hence, it is very important that the client should be able to verify the integrity of the data stored in remote server [12]. The users should be able to detect modification in any part of client’s data, if server modifies; furthermore, the third party auditor must also be able to detect it. This method allows verifying data integrity and its correctness on cloud using Third Party Auditor [13]. It achieves privacy preserving data security using public key based HLA protocol with random masking. And hence, client can easily trust the service provided by cloud, as TPA works on behalf of cloud user. The data will be kept private against the third party auditor, even while verifying the integrity of the client’s data [14] [15].
2) *Cryptographic Techniques for Data Security in Cloud Computing:* Cryptographic technique presents data integrity verification in Cloud Storage without using Trusted TPA (TTPA). TTPA is an independent component which is trusted by both cloud users and service provider. Even though TTPA is reliable, there exist few issues such as leakage of data, scalability, accountability, performance overhead, dynamic data support etc [16]. In cryptographic algorithm, there are two types of key: symmetric key and asymmetric key for encryption and decryption of data. Data security and integrity verification is achieved using Hash Function. Algorithms such as RSA and DES are used for encrypting and decrypting data and then hash code is generated using hash function. Data owner encrypts the file, generates signature using hash function and uploads to cloud. Whenever the owner wants to modify data, a request is send to service provider. Service provider generates hash code data for encrypted file, decrypts it and sends it to data user [16] [17]. Hash functions such as MD5, SHA1, SHA2 and SHA3 are used for data correction and integrity verification.
3) *Three Level Security Systems for Dynamic Group in Cloud:* Cloud computing is a set of network enabled services with guaranteed QoS, inexpensive computing infrastructures on demand with an easy and dynamically scalable. Several techniques are implemented to protect data against unauthorized access. But text based passwords are not enough to solve such problems. Hence there is a need for more secure methods such as Image Based Authentication (IBA). After image authentication, user gets One Time Password (OTP) [18]. Users use this password to access data. This assures high level data security. The aim of Image based authentication is to provide three levels of security. It is a complex study where images are used as passwords and implementation is done using 3 levels of security. In Level 1, Simple text -based password is imposed. In Level 2, Image Based Authentication is imposed and it aims to eliminate attacks such as tempest attack, shoulder attack. In Level 3, the Security System generates a one-time password (numeric password) which will be valid only for that login session. This one time password will be sent to user through his/her email id [19]. This scheme ensures data security at high level as there are three layers/levels of security. It proposes a secure multi-owner data sharing scheme for dynamic group in the cloud.
4) *Data Privacy using Dynamic Reconstruction of Metadata:* Sometimes, there are chances of metadata being leaked to the attackers which could compromise the privacy of user. In this

scheme, Metadata is segregated and put into the cloud [20]. The segregated data are grouped as non-private, partially private and exclusively private depending on data sensitivity. Next step is called as table splitting where the tables are divided horizontally and vertically. This splitting ensures the database normalization. Final step is called as ephemeral referential consonance which involves reconstruction of metadata as and when required by the cloud. This step ensures that data is not leaked from the cloud database before or after table splitting [21].

These are a few schemes that effectively preserve privacy of users' data where their confidential information is stored in the cloud. And, users will be freed from having to worry about data integrity and privacy.

B. Public Auditing Schemes

When Users/Customers store their data in cloud, a TPA will be allotted to check the integrity of data on behalf of users. This process is called Auditing. While maintaining data integrity, it is also important to ensure that data is kept private against TPA.

Few effective public auditing schemes are given below:

1) *Public auditing using Key generation method:* When a third party holds the data, there is a potential lack of control and transparency. This scheme provides efficient privacy preserving and public auditing for data security in cloud computing. It allows TPA to audit various users' data simultaneously (Batch audit). Also, it involves low computation overhead (light weight). This scheme consists of four algorithms [22]. User runs 'KeyGen' algorithm to setup scheme. 'SigGen' is used to generate verification metadata. Server generates a proof of data correctness using 'GenProof' algorithm. Then TPA audits the proof from server using 'VerifyProof' algorithm. There are two phases in this scheme such as setup phase and audit phase [23]. In setup phase, the data owner executes KeyGen and initializes secret and public parameters of the system. Using SigGen, data file is preprocessed to generate the verification metadata. In audit phase, the server should assure that it is retaining the data at any time of audit. To achieve this, TPA sends an audit message to the cloud server. It uses GenProof and VerifyProof algorithm for the data correctness and metadata verification.

This is an effective way of public auditing where four algorithms are used. Here, TPA performs auditing of various users simultaneously. Hence assures time efficiency.

2) *Public Auditing using Hash Message Authentication Code (HMAC) Algorithm:* This scheme ensures that TPA audits the data without making any changes or modification to it and hence data privacy is maintained even against TPA [24]. Cloud data storage service has three components. First component User (U) stores large amount of data in cloud. Second component Cloud Server (CS) manages data storage. Last component Third Party Auditor (TPA) works on behalf of user to access data from Cloud Service Provider (CSP). TPA performs auditing to verify data correctness. TPA ensures data is audited without making any changes to the original data [25]. HMAC is a cryptographic hash function that involves concatenation of hash code, key and the message together. It makes use of hash algorithms such as SHA-1, SHA-256 and MD5 to generate authentication code. Using secret key, authentication code is generated. This code is used to verify integrity of data. It aims to provide protection against man in middle attack [26].

3) *Public Auditing using One Ring to Rule Them All (ORUTA):* It is common that data is not only placed on cloud but also shared among the many users. Due to human errors or hardware/software, data could be easily corrupted or lost. When two users of group exchange information, the identities of users would indicate which users in the group has highest valuable target than others. The proposed scheme solves this problem [27]. Here, homomorphic authenticators are constructed using ring signatures so that TPA will be able to verify integrity users' data of a group without having to retrieve entire data. Also ensures that identity of user is kept private from TPA. During public auditing, ORUTA supports data privacy and dynamic data operations such as insert, update or delete [28]. It has four objectives [29]. First, TPA should be able to correctly detect if there are any changes or modification in data (Correctness). Second, TPA should be able to verify the integrity of data without retrieving entire data (Public Auditing). Third, TPA should ensure that users' identities are not revealed to anyone (Identity Privacy). Fourth, the data verification information generated by one user should not be generated by any other user (Unforgeability). This scheme ensures that users' identity is kept private from each other while exchanging information and also from TPA.

4) *Periodic Sampling Audit Approach:* This scheme provides dynamic audit services for un-trusted and outsourced storage [30]. It aims to reduce the computation costs of third party auditors and storage service providers. The proposed scheme mainly classified into three processes such as tag generation, periodic sampling audit and audit for dynamic operations [31] [32]. In First step, a file is divided into n number of blocks. User uses the secret key to pre-process each file. Then it generates a set of public verification parameters and index hash table which are stored in TPA. Then the verification tags and files are sent to cloud service provider. In Second step, TPA sends a "Random Sampling" message to audit the

availability and integrity of outsourced data by using an interactive proof protocol that is stored in TPA. In Last step, an authorized user can perform various operations such as update, delete and insert using secret key and ensures data/record is not forged [33]. This scheme performs auditing periodically and reduces computation cost of TPA. Hence, ensures data availability, integrity and unforgeability is achieved.

Above mentioned are few schemes which ensure data integrity is achieved while data will be kept private against TPA.

IV. CONCLUSION

Cloud computing is a technology which has been used efficiently by consumers to store and share the data publicly where the security and privacy is the main concern. It reduces users' burden and ensures data integrity. TPA checks the integrity of data periodically on behalf of user and hence assures data correctness. TPA will be completely unaware of users' data during auditing. In this paper, theoretical analysis of various kinds of security threats and various issues that affect the privacy preservation of the data users are done. Also the methods used to solve the security threats are discussed. Different ways to solve the issues that are preventing the privacy preservation are also analyzed. Various types of solutions to overcome these issues are discussed.

ACKNOWLEDGMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India

REFERENCES

[1] Keiko Hashizume, David G Rosado, Eduardo Fernandez Medina and Eduardo B Fernandez, *"An analysis of security issues for cloud computing"*, Journal of Internet Services and Applications, 2013.

[2]Harjit Singh Lamba and Gurdev Singh, *"Cloud Computing-Future Framework for emanagement of NGO's"*, IJOAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[3] Prince Jain, *"Security Issues and their Solution in Cloud Computing"*, International Journal of Computing & Business Research, 2013.

[4] Arijit Ukil1, Debasish Jana and Ajanta De Sarkar, *"A Security Framework in Cloud Computing Infrastructure"*, International Journal of Network Security & Its Applications (IJNSA), Vol.5, September 2013.

[5] Pradeep Kumar Tiwari1 and Dr. Bharat Mishra, *"Cloud Computing Security Issues, Challenges and Solution"*, International Journal of Emerging Technology and Advanced Engineering, Vol 2, Issue 8, August 2012.

[6] Subashini S and Kavitha V, *"A survey on security issues in service delivery models of cloud computing"*, Journal of Network and computer Applications, 2011.

[7] Nikunj Kumar Prof. Priti Sharma, *"Cloud Systems Security Threats and Prevention Mechanisms"*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 4, Issue 5, May 2014.

[8] Kangchan Lee, *"Security Threats in Cloud Computing Environments"*, International Journal of Security and Its Applications Vol. 6, Issue 4, October, 2012.

[9] Aderemi A. Atayero, Oluwaseyi Feyisetan, *"Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption"*, Journal of Emerging Trends in Computing and Information Sciences, Vol 2, October 2011.

[10] Ayesha Malik, Muhammad Mohsin Nazir, *"Security Framework for Cloud Computing Environment: A Review"*, Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, March 2012.

[11] Arumugam.K and Sumathi.P, *"Survey of Cloud Security and Privacy Preservation"*, International of Advanced Information Science and Technology, Vol 28, 2014.

[12] M.Priya, E. Anitha and V.Murugalakshmi, *"Privacy Preserving Public Auditing for Data in Cloud Storage"*, International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, Issue 1, 2014.

[13] K Govinda, V. Gurunathprasad and H. Sathishkumar, *"Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA"*, International Journal of Advanced science and Technical Research, Vol 4, 4 August 2012.

[14] Maha TEBAA, Said EL HAJJI and Abdellatif EL GHAZI *"Homomorphic Encryption Applied to the Cloud Computing Security"*, Proceedings of the World Congress on Engineering, 2012.

[15] Abhishek Mohta, Lalit Kumar Awasti, *"Cloud Data Security while using Third Party Auditor"*, International Journal of Scientific & Engineering Research, Vol 3, Issue 6, June 2012.

[16] Rana M Pir, *"Data Integrity Verification in Cloud Storage without using Trusted Third Party Auditor"*, IJEDR, Vol 2, Issue 1, 2014.

[17] K. Raen, C. Wang, Q. Wang, *"Security Challenges for the Public Cloud"*, Published by IEEE Computer Society, Jan/Feb 2012.

[18] X.Liu,B. Wang,Y.Zhang and J.Yan, *"Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud"*, IEEE Computer Society, vol. 24, June 2013.

[19] V.Sathana and J.Shanthini, *"Three Level Security system for Dynamic Group in cloud"*, International Journal of Computer Science Trends and Technology, Vol 1, Issue 2, 2013.

[20] Waqar A, Raza A et al, *"A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata"*, Journal of Network and Computer Applications, Vol 36, 2013.

[21] T. Jothi Neela and N. Saravanan,*"Privacy Preserving Approaches in Cloud: a Survey"*, Indian Journal of Science and Technology, Volume 6, May 2013.

[22] Almas Ansari and Prof.ChetanBawankar, *"Privacy & Data Integrity for Secure Cloud Storage"*, IOSR Journal of Computer Science, 2014.

[23] Cong Wang, Qian Wang, KuiRen and Wenjing Lou *"Privacy Preserving Public Auditing for Secure Cloud Storage"*, IEEE Transactions on Computers, Vol 62, Issue 2, 2013.

[24] Muralikrishnan Raman and Bharath Elangovan, *"A Metadata Verification Scheme for Data Auditing in Cloud Environment"*, International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, August 2012

[25] Nandeesh.B.B, Ganesh Kumar R, Jitendranath Mungara, *"Secure and Dependable Cloud Services for TPA in Cloud Computing"*, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol 1, Issue 3, August 2012.

[26] S.EzhilArasu, B.Gowri and S.Ananthi, *"Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm"*, International Journal of Recent Technology and Engineering, Vol 2, Issue 1, 2013.

[27] Q. Zheng and S. Xu, *"Secure and Efficient Proof of Storage with Deduplication"*, Proc. ACM Conference on Data and Application Security and Privacy (CODASPY), 2012

[28] Boyang Wang and Baochun Li, *"Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud"*, IEEE Transactions On Cloud Computing, 2012.

[29] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, *"LT Codes based Secure and Reliable Cloud Storage Service"* in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2012.

[30] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-JoonAhn, Hongxin Hu, Stephen S. Yau, *"Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds"*, ACM, 2011.

[31] Rong C, Nguyen S T et al, *"Beyond lightning: A survey on security challenges in cloud computing"*, Elsevier, Vol 39(1) 2013.

[32] Indrajit Ray and K.Belyaev, *"Secure Logging As A Service-Delegating log management to the cloud "*, IEEE Systems Journal, June 2013.

[33] Vikram.J, M.Kalimuthu, *"A Comparative Study on Privacy-Preserving Public Auditing for Secure Cloud Storage"*, IJIRCCE, Vol. 2, Issue 11, November 2014.