International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

Survey on Privacy Preserving Issues with Possible Solutions in Cloud Computing

Mr. Korde S. A., Miss. Tingare B.A.
korde.santosh@gmail.com ,bhagyashreetingare@gmail.com

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. Cloud computing is a natural evolution for data and computation centers with automated systems management, workload balancing, and virtualization technologies. 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. Lot of investigation has been made to identify the issues with these cloud service providers and cloud security. In this paper, the authors discuss security issues, privacy and control issues, accessibility issues, confidentiality, integrity of data and many more for cloud computing. Current solutions for these security risks are also discussed.

Keywords*:* Cloud storage, Cloud computing models, Security issues, Privacy Preserving Schemes.

1. 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:* Itmakes 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.

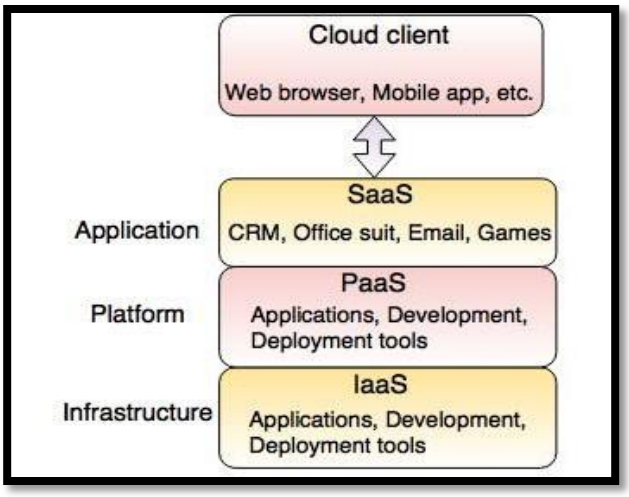

Fig No: 1 Cloud Computing Models

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, Enduser, 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. [25]

2. PRIVACY IN CLOUD STORAGE

Cloud provides many services like in online marketing, banking and payment, healthcares, social media as per use of personal information. Those privacy-sensitive data are residing in the other side of the globe. This movement highlights concerns on privacy and security in the cloud like how privacy of users is protected and perceived. For these growing privacy treats, many technologies have been proposed. The governments in the world are preparing lawful frameworks to protect security and privacy. A. Something About Privacy Privacy is the preservation of the personal information of the cloud user. The cloud user can store their data and be worry free of the data security. Privacy means that the person to be free from all disruption. The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA) define about the privacy as: "Privacy is the right and obligation of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information". B. Issues in cloud storage about Privacy and security Considering the privacy risk of user data in cloud storage, it is important as privacy threats vary according to what type of cloud scenario. The following issues are addressed in cloud storage: The treats against information assets residing in cloud computing environments.

- The types of attackers and their capability of attacking the cloud.
- The security risks associated with the cloud, and where relevant considerations of attacks and Countermeasures.
- Emerging cloud security risks.
- Some example cloud security incidents.

Some other issues like lack of training and expertise, unauthorized secondary usage, complexity of regulatory compliance, lack of user control, addressing transborder data flow restrictions, legal uncertainty, compelled disclosure to the government, data accessibility, location of data, transfer and retention, data security and disclosure of breaches.[22][23][24]

3. PRIVACY PRESERVING 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. [25]

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. [25]

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][25].

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. [25]

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.[25]

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][25].

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.

4. 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. 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.

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] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42
[23] Mohammed, A., AlSudiari, T., & Vasista, T. G. K. 2012. Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications.Advanced Computing: An International Journal (ACIJ), 3 (2), 159-169.
[24] Salve Bhagyashri , Prof. Y.B.Gurav, "A Survey on Privacy-Preserving Techniques for Secure Cloud Storage", IJCSMC, Vol. 3, Issue. 2, February 2014, pg.675 – 680.
[25] Pooja HP, Nagarathna N, " Privacy in Preserving Issues and their Solutions in cloud Computing - A Survey"