Privacy-Preservation and Public Auditing for Cloud Data - A Survey

S Archana[1], Ananthi J[2]

[1]PG scholar, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India

[2]Assistant Professor, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India

Abstract: ***Cloud Computing is a class of network based computing over Internet. Cloud data services not only stores data in the cloud but also shares across multiple users. The integrity of cloud data is subjected to reluctance due to failure of either hardware or even software and also human errors as well. Several mechanisms have been designed in order to allow both the data owners as well as the public verifiers to audit cloud data integrity efficiently without retrieving the entire data from the cloud servers. A Third Party Auditor (TPA) will perform integrity checking and the identity of the signer on each block in shared data is kept private from them. In this paper, a brief survey regarding the various mechanisms for privacy preservation and public auditing of cloud data is done and analysed.***

Keywords: Public auditing, Shared data, Cloud Computing

1. Introduction

The meaning of Cloud Computing is the delivery of many different types of services and various applications from the internet. The fact is that in many cases the devices used to access these services and applications do not require any other special applications requirements. Cloud computing has gained a lot of importance in the current I.T. world. It has become one of the most unique developments in the computer world just after the internet connectivity. Cloud computing is the use of the Internet for the tasks performed on the computer and it is envisioned as the next generation architecture of IT enterprise. It is a common way for the users to utilize the cloud storage services and to share the data with others in a group, as data sharing has become a standard feature in most of the cloud storage offerings, like for example the Dropbox, Google Drive, iCloud, etc.

Security in cloud is one of the major issues which is been handling till now. Privacy and Integrity is yet most important area to be considered. To protect the integrity of data in an untrusted cloud, a number of mechanisms have been proposed. One of the most significant and common features of these mechanisms is their ability to allow not only the data owner, but also a public verifier, such as a third party auditor (TPA), to check data integrity in the cloud without downloading the entire data, referred to as public auditing. Most of the privacy techniques are being implemented by public auditing technique. There are still some very previous works which did not support public auditing. Hence it is the need of the hour to implement security in cloud data.

1.1 Cloud Services

There are various web services which are being delivered from the cloud [7]. Software can be purchased and installed on the personal computers is one of the traditional models of software distributions. This can be called as Software-as-a-Product. Applications can be hosted by any vendors or any service providers and can be made available to the customers over the Internet. Such a model is called Software-as-a-Service (SaaS). Since the web service supporting technologies are being developing, SaaS is becoming an increasingly important delivery model and new developmental approaches become popular. SaaS can also be affiliated with a “pay-as-you-go” subscription licensing model. In the mean time, broadband service has become available to the users. Communication-as-a-Service (CaaS) is yet another important services provided by cloud which is provided by any enterprise communications solution. Providers of this type of cloud-based solution is known as CaaS vendors who are responsible for the management of hardware and software required for delivering Voice over IP (VoIP) services, Instant Messaging (IM), and video conferencing capabilities to their customers. Infrastructure is also a service in cloud land, and there are many variants on how infrastructure is managed in cloud environments. Infrastructure-as- Service (IaaS) is the delivery of computer infrastructure mainly any platforms or virtualization environments as a service to the users. When vendors deliver IaaS, it depends heavily on modern on-demand computing technology and high-speed networking. Monitoring-as-a-Service (MaaS) is the provisioning of security, mainly on the business platforms that uses the Internet for conducting business. Cloud computing also includes platforms for building and running custom web-based applications, and this concept is known as Platform-as-a- Service (PaaS). PaaS developers are concerned on the web based development and generally do not consider what is the operating system which is being used. PaaS services allow users to focus on innovations rather than the complex infrastructure.

An overall view of the various service models is as given in figure 1. The user would use the various service models as per their need. Hence security and integrity assurance is as well very important in every model of cloud services.

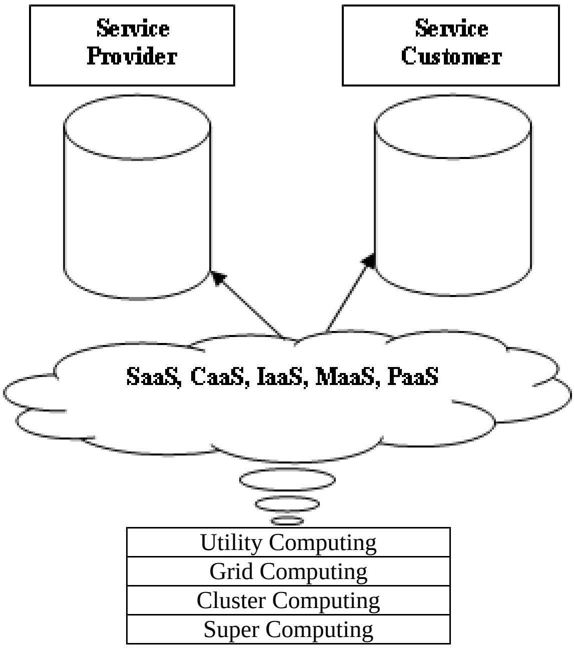

Figure 1: Building blocks to the cloud

1.2 Privacy and Public Auditing

Security and privacy is one fundamental obstacle for the success of cloud computing. Privacy is a critical concern with regard to the cloud computing. This is due to the fact that customers' data and business logic both reside in distrusted cloud servers, which are owned and maintained by the cloud provider. Therefore, there are potential risks to the various confidential data like the financial data, health records and personal information like personal profile since these may be disclosed to public or business competitors. Privacy has been an issue of the highest priority within other security issues.

Privacy-preservability is one of the core attribute of privacy [8]. A few security characteristics may directly or indirectly influence privacy-preservability, including confidentiality, integrity, etc. Evidently, in order to keep private data from being disclosed, confidentiality becomes an unavoidable attribute, and integrity ensures that data or computation is not corrupted, which somehow preserves privacy. On contrary, Accountability may undermine privacy due to the fact that the methods of achieving the two attributes usually may conflict.

1.3 Security Privacy

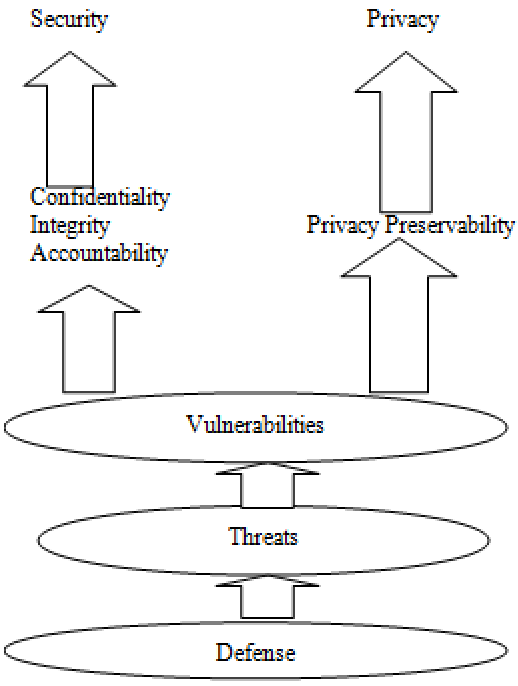

Figure 2: Ecosystem of Cloud Security and Privacy

2. Techniques Used for Public Auditing

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. The TPA can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform, and even serve for independent arbitration purposes. In a word, enabling public auditing services will play an important role for this cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud. Recently, the notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. A brief survey of various techniques has been discussed further.

A Privacy Preserving Policy-Based Content Sharing in Public Clouds is implemented using a Broadcast Group Key Management (BGKM) scheme[5]. An attribute based access control mechanism is developed whereby a user is able to decrypt the contents if and only if its identity attributes satisfy the content provider's policies, whereas the content provider and the cloud learn nothing about user's identity attributes. The mechanism is fine-grained in that different policies can be associated with different content portions. A user can derive only the encryption keys associated with the portions the user is entitled to access. But in this approach the size of the encrypted database is not constant with respect to the original database size. Redundant encryption of the same record is required to support attribute-based access control policies (acps) involving disjunctions.

Another public auditing mechanism for shared data is implemented with efficient user revocation in the Cloud[3]. This mechanism implements integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, the cloud can perform to re-signing of blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, the mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. But with this mechanism if a revoked user is able to collude with the cloud, which possesses a re-signing key, then the cloud and that revoked user together can be able to easily reveal the private key of an existing user. To overcome this limitation, some proxy resignature schemes with collusion resistance in which one can generate a re-signing key with a revoked user's public key and an existing user's private key, can be used. Unfortunately, how to design such type of collusion resistant proxy re-signature schemes while also supporting public auditing, that is, blockless verifiability and non-malleability remains to be seen.

Yet another technique is where a secure multiowner data sharing scheme is used for dynamic groups in the cloud[4]. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users. But unfortunately this mechanism is not highly efficient in terms of accuracy.

Public Auditability and Data Dynamics for Storage Security in Cloud Computing[6] can as well be enabled by identifying the difficulties and potential security problems with fully dynamic data updates. In particular, to achieve efficient data dynamics, proof of storage models can be enhanced by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, bilinear aggregate signatures can be used so that a TPA can perform multiple auditing tasks simultaneously. But unfortunately with this mechanism only private data can be verified and hence this mechanism is not efficient. Also high amount of storage space is required.

Assurance to the users of the correctness of the data in cloud is an important concern to be addressed. As the data is physically not accessible to the user, the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. Also checking the integrity of data without downloading them, known as public auditing, is as well an effective method. There are various techniques which are being used for privacy preservation and public auditing. Each one is better than other but at the same time all these mechanisms have both advantages as well as disadvantages. Hence it is very much essential to choose an appropriate method for performing public auditing so that efficient integrity check without losing the identity privacy can be done. A comparison study of these mechanisms will make it simple to choose the best mechanism to perform auditing as well as integrity check.

3. Applications

Role of Cloud Computing is very remarkable and it is one of the emerging technologies in the world of computers. Cloud run on a shared data centers virtually, hence the name Cloud Computing. Cloud computing can help facilitate easier access and distribution of information among the various medical professionals who would come in contact with individual patients. Cloud Computing is used in almost all fields related to the computer trends. Cloud computing are used in Entertainment, Medical, Military Operations, Security related issues, Business Organizations, finance etc. Since these are being widely used all over, security and privacy issues are widely needed to be concerned.

4. Conclusion

A detailed survey on ensuring the correctness of users' data in the cloud and integrity of data is done which includes privacy preserving public auditing mechanisms for shared data in the cloud. A public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, batch auditing can as well be done. Data storage correctness, allow the authenticated user to access the data and data error localization. Highly efficient and resilient against malicious data modification attack and server colluding attacks can support security and efficient dynamic operations on data blocks.

References

[1] Zhifeng Xiao and Yang Xiao, *Senior Member, IEEE*, "**Security and Privacy in Cloud Computing**", IEEE Communications Surveys & Tutorials, vol. 15, no. 2, second quarter 2013.

[2] Zahir Tari, RMIT University,"**Security and Privacy in Cloud Computing**", IEEE Cloud Computing published by the IEEE Computer Society 2014.

[3] B. Wang, B. Li, and H. Li, "**Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud**," IEEE Trans. Services Computing, 20 Dec. 2013

[4] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, "**Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud**", IEEE Transactions On Parallel And Distributed Systems, VOL. 24, NO. 6, June 2013.

[5] Mohamed Nabeel, Member, IEEE, Ning Shang, and Elisa Bertino, Fellow, IEEE, "**Privacy Preserving Policy-Based Content Sharing in Public Clouds**", IEEE transactions on knowledge and data engineering, November 2013.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "**Enabling Public Verifiability and Data Dynamic for**

Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security, 2013.

[7] John W. Rittinghouse James F. Ransome, "**Cloud Computing Implementation, Management, and Security**", CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business.

[8] http://techatftc.wordpress.com/2012/05/15/what-does-it-mean-to-preserve-privacy/

Author Profile

Ms. Ananthi J received B.E(CSE) from Government College of Engineering and Technology, Coimbatore in the year 2009 and M.E(CSE) from College of Engineering , Guindy, Chennai in 2011. Presently she is working in Hindusthan College of Engineering and Technology, TamilNadu, India as Assistant Professor in Department of Computer Science and Engineering. She has 3 years of teaching experience. Her research interests are Data Mining and Cloud Computing.

S Archana received the B Tech Degree in Computer Science and Engineering from Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India affiliated to University of Calicut in 2013 and is currently pursuing M.E degree at Hindusthan College of Engineering and Technology, Coimbatore, TamilNadu, affiliated to Anna University. Her fields of interest are Cloud Computing and Data Mining.