SURVEY ON SECURING OUTSOURCED STORAGES IN CLOUD

Blessty Sweetline.T

[1]*M.Tech student, CSE department, SRM University, Tamil Nadu, India*

Abstract

Cloud computing is one of the buzzwords of technological developments in the IT industry and service sectors. Widening the social capabilities of servicing for a user on the internet while narrowing the insufficiency to store information and provide facilities locally, computing interests are shifting towards cloud services. Cloud services although contributes to major advantages for servicing also incurs notification to major security issues. The issues and the approaches that can be taken to minimise or even eliminate their effects are discussed in this paper to progress toward more secure storage services on the cloud.

Keywords: *Cloud computing, Cloud Security, Outsourced Storages, Storage as a Service*

----------***----------

1. INTRODUCTION

Cloud computing is one among the upcoming technologies and delivers a solution for the limited storage and services available in the IT industry. Cloud computing can be defined as computing services in terms of Infrastructure, Software and Platform clouding over the internet to cater to the outgrowing needs of an organisation or an individual. Cloud services are in three layers: Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). A further classification of IaaS is Storage as a Service (StaaS).

While outsourcing local information to the cloud to relieve the local resources of space and power consumption and storing them on the cloud is an attractive alternative it imposes security concerns. Security for outsourced storages is one of the predictable research concerns for the future.

2. STORAGE AS A SERVICE

Cloud storage can be provided in all the three types of clouds, being private, public and hybrid. Storage in the cloud usually refers to information or data storage. Storage as a Service (StaaS) [3] is made available by Cloud Service Providers (CSP) who own huge servers to store the data. These CSP however store the data outside the premises of the individuals control on the data. CSP take note of the security and privacy of the information stored though not completely. StaaS can be considered like having a big hard drive in the sky. Services can allow users to store, share and sync data in the cloud. Some examples for such cloud storage services are Dropbox, SkyDrive and Amazon S3 services.

3. SECURITY ISSUES IN OUTSOURCING DATA

Security is a troubling concern for cloud computing. As with all the networks, the broader an environment grows into the more it gets vulnerable to security leaks and cloud is no exception to it. Some of the security issues to be addressed are listed below:

3.1 Trust

Trust between the Service provider and the customer is one of the major risks. There is no way for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of insider attacks. This is a major issue and has received strong attention by companies. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do. However, there is currently no clear format for the SLA, and as such, there may be services not documented in the SLA that the customer may be unaware that it will need these services at some later time.

3.2 Infrastructure Security

Cloud computing involves a combination of computing devices which might be vulnerable to internal and external attacks similar to personal systems. Providing security to the cloud infrastructure in terms of storage is of need.

3.3 Data Integrity

Cloud storage can be an attractive means of outsourcing the day-to-day management of data, but ultimately the responsibility and liability for that data falls on the company that owns the data, not the hosting provider. As data is stored by a third party, it is necessary to check if the data is valid or trustworthy.

3.4 Data Privacy

It is important to gauge how safe your data is in the cloud! Cloud Service Providers might act unfaithfully towards the information provided by the users. It is necessary therefore to ensure privacy for the user's data such that it is not being mined by other sources for marketing and advertising purposes.

3.5 Timely Anomaly Detection

When data is updated in the cloud, detecting anomalieswhich do not conform to an expected pattern or other items in adataset should be insured resulting in a statistically significant increase in data accuracy.

3.6 Data Loss

Accidental deletion happens a lot more often than people think and it's not the only way to lose data. A bad sync, natural disaster or system failure can turn data into memories at the drop of a hat. So it is necessary for cloud services to keep back up in place.

4. METHODOLOGIES FOR SECURING CLOUD STORAGES

4.1 Cryptographic Technologies

Hash functions and signature schemes [4] are deployed to check the correctness of the data disposed to the cloud. Integrity verification of the data is made possible by downloading the copy of data. Since the data is not placedin the hands of an outsider, data privacy is also adhered to in these cryptographic schemes. However,these traditional schemes introduce overhead at the client for computing the hashes as well as issues including requirement of a local copy and increasing communication costs.

4.2Query Integrity

Query integrity [8] is ensured to check if the data returned by the service provider are correct as well as complete. Earlier approaches allowed auditing for results sent back by the serverat the client side. Xie et al proposed that instead of auditing results sent by the server, a small amount of records can be inserted automatically into an outsourced database and an audit can be carried by analysing the inserted records in the query results. Integrity auditing uses deterministic functions to embed fake tuples in the outsourced data. Integrity auditing will introduce query overhead at the server side as the additional fake tuples need to be processed.

4.3 Logcrypt

The scheme in [9] extends forward MAC strategy to Public Key Cryptography (PKC) domain to achieve public verifiability. Logcrypt provides strong cryptographic assurances that data stored by a logging facility before a systemcompromise cannot be modified after the compromisewithout detection. The system supports forward secrecy as well as verifiability without the ability to forge entries.Despite the fact of being an innovative way of forward security for audit logs, it still incurs significant storage and communication overheads due to the requirements of storing and transmitting an authentication tag for every log entry or logging period.

4.4 Blind Aggregate Forward (BAF)

BAF [2] as proposed byYavuz.A.A and Ning.P provides security for audit logs. Audit logs require forward security i.e. attacker cannot forge log entries accumulated before compromise. BAF does not require online trusted third party support and provides publicly verifiable forward secure and aggregate signatures with low or near zero computational costs. BAF is an ideal solution for secure logging but BAF does not use the time factor to be publicly verifiable, and therefore achieves limited verification.

4.5Proofs of Retrievability

Exploiting data encryption before outsourcing is one approach to weaken the data privacy concern. A POR [11] may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file (or bitstring) F. POR accomplishes in providing checks without users having to download the files themselves. Yet, it does not prevent data from privacy attacks but just reduces it to the key management. Potential exposure of decryption keys yields to the problem of data leakage to external sources.

4.6Provable Data Possession

Atenieseet al. proposed a model [11] that generates probabilistic proofs of possession by sampling random sets of blocks from the server which drastically reduces I/O costs. The provable data possession techniques verify that the server possesses the original data without retrieving it. This requires the server to access the entire file, which is not feasible when dealing with large amounts of data.

4.7Efficient Provable Data Possession

Meng et al. proposed a cooperative PDP [6] scheme in hybrid clouds to support scalability of service and data migration, in which we consider the existence of cloud service providers tocooperatively store and maintain the client's data. The overheads are reduced when the values of optimal value are increased. Hence, it is necessary to select the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers. But it is critical to select the number of sectors for each and every block.

4.8Public Verifiability

To ensure security for cloud storages, a public verifiable authority delegated as a Third party Auditor is proposed in this method [7] by Qian Wang et al.Public verifiability dispatches integrity verification checks to the TPA relieving the users' of communication overhead and computation resources required. The system however does not relinquish to the need of ensuring privacy of the data.

4.9Auditing Online Storages

Auditing of Online Service Providers (OSP) is suggested in [1], enabling a third-party auditor to assess and expose risks, thereby allowing end users to analyse and choose rationally between competing services. Though auditing complies to increase the efficiency of insurance-based risk mitigation, this method serves as a solution only for online service-oriented transactions.

4.10Privacy-Preserving Public Auditing

An effective Third Party Auditor (TPA) for auditing data in cloud is used in the system [10] proposed by Wang et al rather than the end users performing the audit. The public auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. Public Key based Homomorphic Linear Authenticator (HLA) scheme is used. Scheme involves privacy-preserving auditing protocol and batch auditing. This scheme only works for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up.

4.11Dynamic Audit Services

Dynamic Audit Services [5] proposed by Yan Zhu et al. provides a combinatory solution for data integrity and data privacy. The system also supports detection of anomalies in data and dynamic auditing for the dynamic data operations that take place in the cloud storages. Though the service proposes security with auditing capabilities, it is vulnerable to attacks during data outsourcing.

5.PREDICTIONS FOR CLOUD SECURITY IN THE FUTURE

Mass data breaches at Twitter, Facebook, Adobe and The New York Times (just to name a few) were nightmares that raised the profile of data security — particularly in the cloud — as a recurring topic of conversation in the boardroom. No doubt today's needs may define many of tomorrow's innovative technologies. Some of the suggestions that can be predicted to be carried out in the face of cloud security can be providing encryption keys to end users that are revocable, protecting data from intrusion attacks, data theft and DOS attacks.

CONCLUSIONS

Cloud computing as it blooms in the IT industry, allows security concerns that need to be noted to sprout along with it. Cloud storage enables users to make use of the space available in the cloud, freeing up local storage resources.It is indeed critical to understand the issues posed on such outsourced storages which are briefed in this paper. The paper also gives insight into the methodologies available for providing security for the outsourced data with their pros and cons. The survey brings to light further security concerns that are evolving and need to be catered to.

REFERENCES

[1].M. Shah, M. Baker, J. C. Mogul, and R. Swaminathan. "Auditing to keep online storage services honest", In Proc. of HotOSXI.Usenix, 2007

[2]. Yavuz.A.A and Ning.P,"BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proceedings of the. Ann.Computer Security Applications Conference (ACSAC), pp. 219-228, 2009

[3].GurudattKulkarni, Ramesh Sutar, JayantGambhir, "Cloud Computing-Storage as Service," International Journal of Engineering Research and Applications (IJERA) ,Vol. 2, Issue 1,Jan-Feb 2012, pp.945-950

[4].SubraKumaraswamy , ShahedLatif Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) Tim Mather ,Ch no:4, pp 61-71, Published by O'Reilly Media Inc.Publication Date: October 5, 2009 , ISBN-13: 978-0596802769, Edition: 1.

[5].Yan Zhu, Gail-JoonAhn, Hongxin Hu, S. S. Yau, H. G. An, Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227-238, April-June 2013, doi:10.1109/TSC.2011.51

[6].Zhu.Y, Wang.H, Hu.Z, Ahn.G-H, Hu.H, and Yau.S.S, "Efficient Provable Data Possession for Hybrid Clouds," Proceedings of the 17th ACM Conference on Computer and Communication Security, pp. 756-758, 2010.

[7].Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370

[8].Xie.M, Wang.H, Yin.J and Meng.X, "Integrity Auditing of Outsourced Data" Proceedings of the 33rd International Conference on Very Large Databases (VLDB), pp. 782-793, 2007.

[9].J. E. Holt, "Logcrypt: forward security and public verification for secure audit logs," in ACSW Frontiers '06: Proceedings of the 2006 Australasian workshops on Grid computing and e-research. Australia: Australian Computer Society, Inc., 2006, pp. 203–211.

[10].Wang.C, Wang.Q, Ren.K and Lou.W, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" Proceedings of the IEEE INFOCOM, pp. 1-9, 2010.

[11].A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

[12].Ateniese.G, Burns.R.C, Curtmola.R, Herring.J, Kissner.L, Peterson.Z.N.J, and Song.D.X, "Provable Data Possession at Untrusted Stores," Proceedings of the 14th ACM Conference on Computer and Communication Security, pp. 598-609, 2007.