Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Secure Overlay Techniques for Cloud Storage

Dathi Soniya.M*, Roshni Thanka.M

Department of Computer Science and Engineering,
Karunya University, India

Abstract— Cloud computing does an all time existing data storage that stores and provides data in large amount also at any time. The storage of data however has some kind of security issues in accessing the authorized data. Some of the data in the cloud should be deleted for certain reasons to maintain confidentiality. And many other issues are to be overcome by the cloud. There are certain techniques discussed in this paper to address the problems in the cloud communication. We get an idea of the available methods in which the data can be secured. Anyway each architecture has its own shortcomings. But without these techniques, it is difficult to maintain a good client-server storage mechanism in the cloud computing.

Keywords— Cloud computing, Data, Access control, Security, Cloud storage.

I. INTRODUCTION

Cloud computing is an emerging technology which branches into various areas. Internet is a collection of networked computers. Similarly Cloud is a distributed system that consists of a collection of inter-connected and virtualized computers which are presented as unified computing resources. The ultimate aim of Cloud computing is to share the data, services and also resources among its users. It provides the users to make use of many applications. It believes in improving the utilization rate of the computers and decreasing the energy consumption. The mode of using is pay per usage. We will pay only for whatever resources we consume. The services provided by cloud computing is mainly divided into three categories namely,

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

The cloud environment is a large open distributed system. It is important to preserve the data, as well as, privacy of users.

Access Control methods ensure that authorized user's access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security.

One specific issue is that upon requests of deletion of files, cloud storage providers may not completely remove all file copies (e.g., cloud storage providers may make multiple file backup copies and distribute them over the cloud for reliability, and clients do not know the number or even the existence of these backup copies), and eventually have the data disclosed if the encryption keys are unexpectedly obtained, either by accidents or by malicious attacks.

II. EXISTING TECHNIQUES IN CLOUD STORAGE

A. *RACS: Redundant Array of Cloud Storage*

RACS is a middleware that extends the load of stored data clearly over multiple data providers. RACS is placed as a proxy that performs between the client and the multiple repositories [1]. RACS is likely to be performed parallel communication in a distributed environment with multiple proxies. It can also be run on multiple proxies with the same set of repository using policies.

This technique is mainly introduced to avoid vendor lock-in and also to reduce the cost of switching providers. The provider failures are tolerated. This technique is simple and easy to work with. Since, all data must pass through a RACS proxy either for encoding or decoding, a single proxy could easily become a bottleneck [1].

B. *SOS: Secure Overlay Services*

An architecture called Secure Overlay Services (SOS) is proposed intentionally to prevent DOS attacks. The two principles behind this technique are:

- The elimination of communication pinch points, that represent attractive DoS targets, using the filtering
- The ability to make progress from arbitrary failures within the forwarded infrastructure

In this technique, the incidence of attacks may be reduced by not allowing the hackers to perform any kind of denial of service attacks with the cloud [3]. Secure overlay services reduce the probability of successful attacks. Implementing an SOS infrastructure is fairly straightforward and can be done using exclusively readymade protocols and software.

It is hard to solve DDoS problem completely. The ideal solution could be very complicated. It might need an integrated solution. It's unclear about the optimal integration [3].

C. *Vanish*

Vanish ensures that all the copies of certain data become unreadable after a user specified time, even if an attacker obtains both a copy of that data and the user's cryptographic keys. A system meets this challenge through cryptographic techniques using the global-scale, P2P, Distributed Hash Tables (DHTs) [4]. User creates Vanishing Data Object (VDO) for each data and the copies are stored nowhere. In this technique, the data stored in the cloud are deleted permanently after a certain period of time with the knowledge of the user who created it. Vanish causes susceptible information, such as emails, files, or text messages, to destroy itself, without any action on the user's part and without any centralized or trusted system.

It is practical to use and also meets the privacy preserving goals. It is broadly applicable in today's web-centered world [4]. The DHTs are having a property of making place for new data instead by discarding older data after s set of time. They would be expensive. Large DHTs are required.

D. FADE

FADE is a secure overlay cloud storage system that ensures file assured deletion. FADE is a practical, implementable, and readily deployable cloud storage system that focuses on protecting deleted data with policy-based file assured deletion [11]. FADE is built upon standard cryptographic techniques, such that it encrypts outsourced data files to guarantee their privacy and integrity, and most importantly, assuredly deletes files to make them unrecoverable to anyone (including those who manage the cloud storage) upon revocations of file access policies [11].

They are practical to use. The data owners can be sure of the deleted file [11]. Only the deletion part of the file is considered, not the accessing of data. The operations are performed on a per-file basis.

E. *Sybil Attacks*

These Sybil attacks are explored to defeat vanish implementation and to mention the drawbacks of the large DHTs. These attacks work by continuously moving forward the DHT (Distributed Hash Table) and each value is stored before its expiration [6]. They can efficiently recover keys for more than 99% of vanish messages. All operations are performed using simple RPC commands that are sent directly to the remote peer in a single UDP packet. This technique proposes to use decentralized key management with the existing peer – peer DHT systems.

They recover the keys to almost all Vanish data objects at low cost. The Vuze DHT replicates entries twenty times and actively creates replicas periodically [6]**.** Network transfer is the limiting cost, but it is not the case with memory or CPU. The amount of traffic used for the attack is very difficult to estimate without participating in the real network.

F. *Plutus*

Plutus aims to provide strong security even with an untrusted server. The main feature of Plutus is that all the data are stored encrypted and all key distribution is handled in a decentralized manner [13]. All cryptographic and key management operations are performed by the clients, and the server writes very little cryptographic overhead. Mechanisms that Plutus uses to provide basic file system security features are: to detect and prevent unauthorized data modifications, to differentiate between read and write access to files and to change user's access privileges [13].

This technique, Plutus enables secure file sharing without placing much trust on the file servers. In particular, it makes use of cryptographic primitives to protect and share files [13].

It provides protection against data outflow attacks on the physical device. It allows users to set arbitrary policies for key distribution. It enables better server scalability. Aggregating keys - reduces the number of keys that users need to manage, distribute, and receive. Most of the complexity of the implementation is at the client-side.

III. CONCLUSION

Cloud Computing is an emerging computing paradigm, allows users to share resources and data from a puddle of distributed computing made as a service over Internet. Though Cloud provides payback to users, security and privacy of stored data are still major issues in cloud storage. Cloud storage is greatly more advantageous than the earlier traditional storage systems especially in scalability, cost reduction, portability and functionality requirements. This paper presented a survey on secure overlay techniques for cloud storage in Cloud Computing. The study of the literature survey gives clear knowledge in depth about the cloud storage and the securities required to overcome certain limitations. Few papers that work on the integrity and security of data in cloud are discussed, however not all the papers concentrate on all the issues at the same time. Several storage techniques that provide security to data in cloud have been discussed in detail along with their advantages and limitations.

REFERENCES

[1] Abu-Libdeh, L. Princehouse, and H. Weatherspoon, (2010) "RACS: A Case for Cloud Storage Diversity," Proc. ACM First ACM Symp. Cloud Computing (SoCC).

[2] Boldyreva, V. Goyal, and V. Kumar, (2008) "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS).

[3] Angelos D. Keromytis, Vishal Misra, Dan Rubenstein, (2002) "SOS: Secure Overlay Services,"http://www.cs.columbia.edu/~angelos/Papers/sos.pdf.

[4] Geambasu, T. Kohno, A. Levy, and H.M. Levy, (Aug. 2009) "Vanish: Increasing Data Privacy with Self-Destructing Data," Proc. 18th Conf. USENIX Security Symp.

[5] Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, (2008) “Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf. Security and Privacy in Comm. (SecureComm).

[6] Wolchok, O.S. Hofmann, N. Heninger, E.W. Felten, J.A. Halderman, C.J. Rossbach, B. Waters, and E. Witchel, (2010) “Defeating Vanish with Low-Cost Sybil Attacks against Large DHTs,” Proc. 17th Network and Distributed System Security Symp. (NDSS).

[7] Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, (Apr. 2010) “A View of Cloud Computing.” Comm. ACM, vol. 53, no. 4, pp. 50-58.

[8] Vrable, S. Savage, and G.M. Voelker, (2009) “Cumulus: Filesystem Backup to the Cloud,” ACM Trans. Storage, vol. 5, no. 4, article 14, Dec.

[9] Stallings. Cryptography and Network Security. Prentice Hall, (2006).

[10] Perlman, “File System Design with Assured Delete, (2007)” Proc. Network and Distributed System Security Symp. ISOC (NDSS).

[11] Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman, (2010) “FADE: Secure Overlay Cloud Storage with File Assured Deletion,” Proc. Sixth Int’l ICST Conf.Security and Privacy in Comm. Networks (SecureComm).

[12] Perlman, C. Kaufman, and R. Perlner, (2010) “Privacy-Preserving DRM,” Proc. Ninth Symp. Identity and Trust on the Internet (IDTRUST).

[13] Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, (2003) “Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc.Second USENIX Conf. File and Storage Technologies.

[14] Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Lui, (2011) “A Secure Cloud Backup System with Assured Deletion and Version Control,” Proc. Third Int’l Workshop Security in Cloud Computing.

[15] Kamara and K. Lauter, (2010) “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security.

[16] Nair, M.T. Dashti, B. Crispo, and A.S. Tanenbaum, (2007) “A Hybrid PKI-IBC Based Ephemerizer System,” Int’l Federation for Information Processing, vol. 232, pp. 241-252.

[17] Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” RFC 5246, Aug. 2008.

[18] THE AMAZON S3 TEAM. Amazon S3 Availability Event: July 20, 2008 [online]. July 2008. Available from: http://status. aws.amazon.com/s3-20080720.html

[19] Goyal, O. Pandey, A. Sahai, and B. Waters, (2006) “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS).

[20] Wang, Q. Wang, K. Ren, and W. Lou, (2010) “Privacy-preserving public auditing for storage security in cloud computing”. In Proc. of IEEE INFOCOM, Mar.

[21] Yun, C. Shi, and Y. Kim, (2009) “On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage”. In ACM Cloud Computing Security Workshop (CCSW), Nov.

[22] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing. http://www.cloudsecurityalliance.org/, April 2009.

[23] Gutmann, (1996) “Secure Deletion of Data from Magnetic and Solid-State Memory,” Proc. Sixth USENIX Security Symp. Focusing on Applications of Cryptography.

[24] Wang, Z. Li, R. Owens, and B. Bhargava, (Nov. 2009) “Secure and Efficient Access to Outsourced Data,” Proc. ACM Workshop Cloud Computing Security (CCSW).

[25] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen, (2010) “Efficient Provable Data Possession for Hybrid Clouds,” http://eprint.iacr.org/2010/234.pdf *CCS’10,* October 4–8.