RESEARCH ARTICLE OPEN ACCESS

Cloud Storage and its Secure Overlay Techniques

Susheel Kumar* Naval Kishore Dogra**
*P.G. Department of computer science, Kamla Nehru College, Phagwara
**P.G. Department of computer science, Kamla Nehru College, Phagwara

Abstract—
In this paper we have tried to explain in detail about cloud storage its need, importance and how much useful it is for the upcoming future. As we know that it provides us flexibility to store and use data to anywhere and from anywhere so it is cost effective and beneficial at all places. 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.

Index Terms— Cloud Storage, cloud services, security, Fade, Plutus.

I. INTRODUCTION

For some computer owners, finding enough storage space to hold all the data they've acquired is a real challenge. Some people invest in larger hard drives. Others prefer external storage devices like thumb drives or compact discs. Desperate computer owners might delete entire folders worth of old files in order to make space for new information. But some are choosing to rely on a growing trend: cloud storage. Instead of storing information to computer's hard drive or other local storage device, it is saved to a remote database. The Internet provides the connection between computer and the database. On the surface, cloud storage has several advantages over traditional data storage. For example, if data is stored on a cloud storage system, user will be able to get to that data from any location that has Internet access. They wouldn't need to carry around a physical storage device or use the same computer to save and retrieve information. With the right storage system, user could even allow other people to access the data, turning a personal project into a collaborative effort.

II. UNDERSTANDING CLOUD STORAGE

- Cloud offers companies and individuals more agility and offers them the ability to store data without the need to use their own servers. By using information technology as a scalable "cloud" of power, the user can respond faster to the ever changing technology found in this industry.
- Cloud is the symbol used in diagrams that represent the Internet in technical drawings. It is starting to revolutionize how people and companies save data and share it with others. It allows Internet users to store unlimited files to a secure data center that is available to anyone that the user authorized access.
- Businesses can treat their technology infrastructure as utilities instead of an asset. This saves them time and money, as well as business space.

III. CLOUD SERVICES

A cloud service provides a remote way of storing all files that provide instant access from a variety of devices. For example,

- A file can be uploaded to cloud account and then retrieved from mobile device if needed access to it while traveling.
- Those files can be shared with friends, family or business associates.
- Anything can be shared securely at any time by granting access to that file and our associate going online to retrieve it whenever and from where ever they choose.

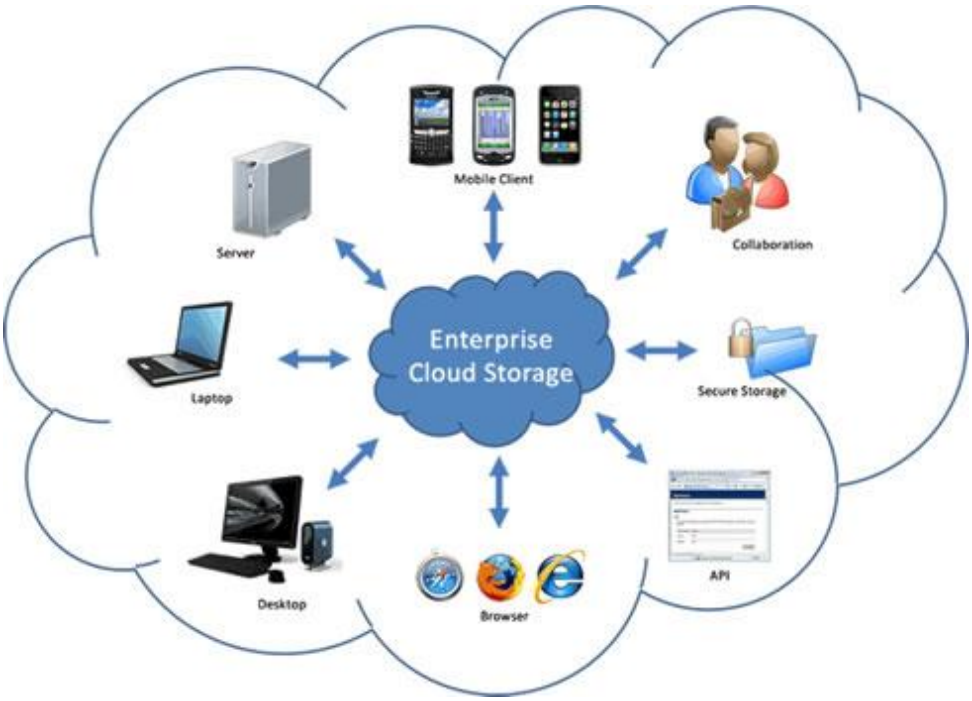

Fig. 1 Cloud Storage

IV. BENEFIT OF CLOUD STORAGE

Cloud Storage can offer individuals and small companies an inexpensive data storage facility without the cost of purchasing their own servers. The data is stored off-site and properly secured, which is required by many small companies, as well as individual business people. The service offers everyone that subscribes to a provider with instant access to all their data from anywhere at any time. It also allows several people to share the same data from anywhere at any time this data storage has no limitations, which is found with individual servers.

- Since individual data storage servers requires a lot of space, the cost of a larger work space is saved and let that area used for a growing business, instead of the growing amount of data accumulated. Instead of paying for more servers to hold every-increasing data and then paying for more space to install those personal servers, Cloud Storage provider can be paid less funds for an unlimited storage area. This is a long-term fix for all data storage needs.
- One other benefit of Cloud Storage is that it can be provided with just as much security features as personal data servers can provide and, sometimes, even more security features. There can be limited people that are authorized to access Cloud Storage data or make that completely public, but that access is controlled. Even though there have been attempts to break into Cloud Storage providers, we hear more about stolen information from private servers. The technology that Cloud Storage providers use to secure their centers and servers is continually being developed to protect their members. This means that these services continue to improve their security technology to enhance the protection of data. Since Cloud Storage is still considered a new technology, there will always be discussions about the problems found with this service. However, no one can say that the benefits do not outweigh the problems. We save on equipment, storage space and can have secured access whenever needed from anywhere in the world, so can our employees.

V. TYPES OF CLOUD STORAGE

- Cloud services have made it possible for users to share, store and host data onto the Internet atmosphere and bypass mainframes, as well as hard drive. This new industry is a combination of synchronized servers that allows carrying out sophisticated computing processes. The system converts important data onto a cloud provider, which can be remotely accessed and cut down the space used on personal hard drive.
- More people are sourcing their data storage to cloud providers because of the cost savings and ease of use, as well as makes accounting, payroll and employee management simpler. Individuals are using cloud services to protect their important data and share videos, as well as pictures with others. It is needed to decide which type of cloud storage fits needs. There are three basic types:
- Private, public and hybrid

Private Cloud Storage: Private cloud storage is exactly what the name says .This system is designed for one person or company that is specific to our needs. These types of cloud storage come in two formats:

- *On-premise and*
- *Externally hosted.*

Both work well, but primarily for businesses, not individuals, unless we are running a smaller home-based company. We have more administrative control and can design the system to what we want it to accomplish in the way of business needs.

Public Cloud Storage: This is a cloud service that requires little administrative controls and can be accessed online by any anyone authorized. We get the same security, but don't need to maintain the system as much as we would with a private cloud. A rigid integration is not needed with business needs or private storage concerns.

Hybrid Cloud Storage: A Hybrid cloud offers a combination of private and public clouds. The features can be customized and the applications are inserted that meet our needs, as well as the resources that work for us. The most important data can be kept on a private cloud, while the less important data can be stored on a public cloud and accessed by a host of people remotely. Data can be stored in an efficient storage environment, which saves time and money.

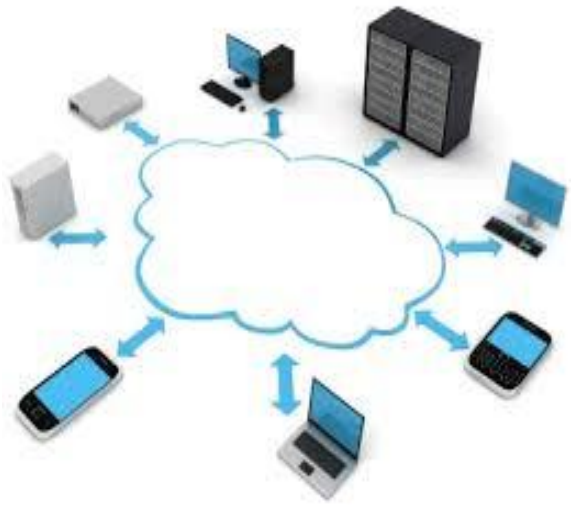

Fig. 2. Storage Types

VI. STORAGE TECHNOLOGIES

There are two types of storage technologies available through cloud storage. These technologies are available for traditional storage systems, also:

- **File Storage:** file storage is the most common type of storage, due to its ease of configuration. Raw files can be stored easily, but there is a lack of customization. File storage is all-encompassing.

Block Storage: block storage creates storage volumes. Each volume can be formatted separately and thus mimic an individual hard drive. Block storage is good for high levels of

storage performance because it's highly customizable, though it requires an attached OS to operate. While block storage is known to offer better performance than file storage, Internet-relative factors such as latency may limit the performance of the storage technology.

VII. TECHNIQUES FOR SECURE CLOUD STORAGE

- **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 [8]. 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 [8].
- **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:
  1. The elimination of communication pinch points, that represent attractive DoS targets, using the filtering
  2. 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 [9]. 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 [9].

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) [10]. 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 [10]. 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.

- **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.

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 [12]. 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 [12]**.** 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.

- **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.

VIII. 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 is a study on storage cloud and its secure overlay techniques 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. Several storage techniques that provide security to data in cloud have been discussed.

References

[1] Greg Schulz, "Cloud And Virtual Data Storage Networking "published -CRC Press, Issue-AUG 2011.
[2] Nabil Sultan, "Cloud Computing for education: A new dawn" International Journal of Information Management 30(2010), pp 109-116.
[3] Ajilth Singh. N and M. Hemalatha, "Cloud Computing for Academic Environment", International Journal of Information.
[4] Velte, "Cloud Computing - A Practical Approach", TMH, 2012.
[5] Buyya ,Selvi, "Mastering Cloud Computing", TMH Pub.
[6] Velte, "Cloud Computing – A practical Approach", TMH Pub.

[7] J. L Nichlson. Cloud Computing: Top Issues for Higher Education. [Online]. Available:http://www.universitybusiness.com/article/cloud-computingtop-issues-higher-education/page/0/3
[8] Abu-Libdeh, L. Princehouse, and H. Weatherspoon, (2010) "RACS: A Case for Cloud Storage Diversity," Proc. ACM First ACM Symp. Cloud Computing (SoCC).
[9] Angelos D. Keromytis, Vishal Misra, Dan Rubenstein, (2002) "SOS: Secure Overlay Services," http://www.cs.columbia.edu/~angelos/Papers/sos.pdf.
[10] 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.
[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] 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).
[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] Rimal, Bhaskar Prasad, Eunmi Choi, and Ian Lumb. "A taxonomy and survey of cloud computing systems." INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on. IEEE, 2009.
[16] Wu, Jiyi, et al. "Recent Advances in Cloud Storage." Proceedings of the Third International Symposium on Computer Science and Computational Technology (ISCSCT'10). 2010.
[17] Wu, Jiyi, et al. "Cloud storage as the infrastructure of cloud computing." Intelligent Computing and Cognitive Informatics (ICICCI), 2010 International Conference on. IEEE, 2010.