SURVEY ON CLOUD STORAGE

Aditi Maulekhi[1]
Department of CSE
MIT ADT University
Pune, India

Khusharth A. Patani[2]
Department of CSE
MIT ADT University
Pune, India

Viral Sangani[3]
Department of CSE
MIT ADT University
Pune, India

Gurveen Singh[4]
Department of CSE
MIT ADT University
Pune, India

Prof. Nikhilkumar Shardoor[5]
Department of CSE
MIT ADT University
Pune, India

Abstract - Now a day's cloud computing has become a trend it is being used in areas like industry, military, education etc. to store larger quantities of data. But, due of insufficient awareness and proper security measures, cloud users suffer because of the security vulnerabilities exposed by the cloud storage. The cloud user and Cloud Storage Provider (CSP) should establish appropriate techniques and follow best practices to overcome the security issues proactively. In this paper various types of cloud storage are proposed like object storage, file storage and block storage. Also the different types of risks in cloud storage have been discussed. This paper will help cloud providers to know that Security of the cloud is a major challenge which has to be addressed.

Index Terms - Cloud service provider(CSP), object storage, block storage, file storage.

I. INTRODUCTION

In the today's world, data security has become one of the most important term for any application. In our day to day life we are using different IOT devices like smart home devices and electronic devices like smart phones, laptops etc. which are using our data. The data which can be used for the development and achievement in a business it has become an unprotected business asset. Hence data security must be a priority and it needs to be secured from unapproved access to ensure the privacy of data and save it from prevent it being altered or revealed. The security can be violated in different manners, for example system failure, theft, inappropriate usage or illegal access. Every time a person uses internet the data security is being compromised. Therefore, to enhance the security of data there are different methods like using strong encryption and decryption for storing and retrieving our data. Use of features like Two Factor Authentication should be promoted among audience.

II. RELATED WORKS

In [1], author proposed a paper on cloud storage facilities about how cloud computing is expanding its reach among people. The authors have focused on structured and unstructured cloud storage types. He has discussed about the issues across cloud vendors. In [2], author proposed paper on overview of data storage in cloud. They have explained the architecture of cloud storage, its various layers and its key issues like data duplication and data organization. They have further explained cloud storage trends like appliances and storage projections. In [3], the authors proposed a survey on cloud storage. The authors have proposed various cloud security services. The authors have explained various goals for cloud storage like data confidentiality, data integrity and availability. They have explained reliability and availability are the major cloud services. In [4], authors proposed a survey paper on cloud computing security. The authors have explained types of cloud public cloud, private cloud and hybrid cloud. Paper has explained types of cloud storage services and various risks of cloud computing.

III. TYPES OF CLOUD STORAGE

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's transferred when demanded with just-in-time capacity and costs, and removes purchasing and handling your own data storage infrastructure. This gives you agility, global scale and durability, with "anytime, anywhere" data access.

Basically there are three types of cloud data storage: object storage, file storage, and block storage.

Object Storage - Applications built in the cloud tend to take advantage of object storage's broad scalability and metadata characteristics. Object storage solutions

like Amazon Simple Storage Service (S3) are perfect for making modern applications from basics that require scale and flexibility, and can also be used to import current data stores for analytics, backup, or archive.

File Storage - Few applications need to acquire shared files and need a file system. This type of storage is often assisted with a Network Attached Storage (NAS) server. File storage solutions like Amazon Elastic File System (EFS) are best for use cases including large content store houses, development environments, media stores, or user home directories.

Block Storage - Other enterprise applications like databases or ERP systems need committed, low latency storage for every host which is similar to direct-attached storage (DAS) or a Storage Area Network (SAN). Block-based cloud storage solutions like Amazon Elastic Block Store (EBS) are equipped with a virtual server and offer the ultra low latency needed for high performance workloads.

IV. SECURITY RISK IN CLOUD STORAGE

A. Data privacy

No one wants to anyone else to access their data without their consent. In cloud the data is stored somewhere else, which might not be possible to know how closed off it is. In order to make sure no one access the data the server where it is stored needs to be maintained. Hence when a person is sending some sensitive data to cloud he needs to be aware that he might be losing privacy controls.

B. Lack of control

By relying on a third party to store data, it removes lot of responsibility from one's shoulders. However, this is, partly good partly bad. On one side person doesn't has to manage his data while on other side someone else is doing it for you. If anything infects your storage provider, like a malware, it will risk your data privacy. You will have to rely on the third party to solve the issue otherwise the attacker might exploit your data.

C. Shared servers

Cloud-based storage systems also use servers to store data, but no one can physically access it. Cloud storage providers don't use separate servers for every user; the space is shared among the customers when needed. A persons may be unknowingly putting his data at risk if some other person too is using the same server and loads any malicious information.

D. Lack of backup services

One of the major drawback of storage systems is that there is no automatic backup functionality. They expect the users to keep backups of data they store on cloud. This issue is not same for every storage provider – some automatically provide backups of user's data. However, the providers who don't provide backups also don't guarantee you a senerafety at the time of sudden data loss.

E. Data leakage

Main work of secure data storage is to make sure no outsider can access your data. Another task is to make sure the important data isn't sent to any outsider (unless user sends it himself). Data leakage can expose business-critical or private data to external sources.

F. Rogue devices

The devices that access your data are also possible sources of danger. Shadow IT is another factor; any device that a worker doesn't register but still uses to access your data can release bad news.

G. APIs and storage gateways

Some businesses use cloud storage APIs or storage gateways to help users transfer their data on cloud. These tools act bridge between the user and the storage provider. They may help your workers access and manage the data on your cloud, but an insecure API or gateway might cause a lot of damage to your data. If you want to use a storage API or gateway, you should choose one that has good and required security features.

VI. CONCLUSION

Cloud computing provides compute, storage and application services among others to users over the Internet. The Cloud is used for various activities but leading among them are computation and storage. Since a cloud infrastructure is a distributed system, storage facilities may be designed like the distributed file system. This paper discussed about various types of cloud storage and the security risks related to cloud. Now a days with increase in growth of clout people are getting more concerned about the security of data so the balance has to maintained. The cloud storage systems are increasing tremendously and in coming future all the shortcomings and risks will be over.

REFERENCES

[1] Dewan, H., & Hansdah, R. C, " A Survey of Cloud Storage Facilities," 2011 IEEE World Congress on Services (pp. 224-231). IEEE.

[2] Odun-Ayo, I., Ajayi, O., Akanle, B. and Ahuja, R. "An overview of data storage in cloud computing," 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) (pp. 29-34). IEEE.

[3] Mishra, B., & Jena, D. (2019). Security of Cloud Storage: A Survey. 2019 International Conference on Information Technology (ICIT).

[4] Kaura, W. C. N., & Lal, A. (2017). Survey paper on cloud computing security. 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).

[5] A. Singh, S. Pasupuleti, Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing, 6th International Conference on Advances in Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India. Procedia Computer Science 93 (2016) 751 – 759

[6] N. Vurukonda, B. Rao, A Study on Data Storage Security Issues in Cloud Computing, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016) , Procedia Computer Science 92 (2016) 128 – 135

[7] L. Stadtmueller, Which Cloud Storage Service Delivers the Performance You Need? Comparing IBM Cloud Object Storage and Amazon S3, An Executive Brief Sponsored by IBM, 2016 Stratecast.

[8]] J. Wu, L. Ping, X. Ge,Y. Wang, J. Fu, Cloud Storage as the Infrastructure of Cloud Computing, 2010 International Conference on Intelligent Computing and Cognitive Informatics. DOI 10.1109/ICICCI.2010.119.

[9] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoik and M. Zaharia, Above the Clouds: a Berkeley view of Cloud Computing, UC Berkeley, Technical Report, 2009.

[10] G. DeCandia et. all., Dynamo: Amazon's Highly Available Key-Value Store, in theProceedings of the 21st ACM Symposium on Operating Systems Principles, Stevenson, WA, October 2007

[11] J. Chris Anderson, J. Lehnardt and N. Slater, CouchDB: The Definitive Guide, OReilly Media, 2010.

[12] Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684-5.

[13] Brian F. Cooper , Adam Silberstein , Erwin Tam , Raghu Ramakrishnan , Russell Sears, Benchmarking cloud serving systems with YCSB, Proceedings of the 1st ACM symposium on Cloud computing, June 10-11, 2010, Indianapolis, Indiana, USA.

[14] T. Ristenpart, "Hey You Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds", Proc. 16th ACM Conf. Computer and Communications Security (CCS 09).

[15] Nagendra, M., Sekhar, "M.C.: Performance Improvement of Advanced Encryption Algorithm using Parallel Imputation.", International Journal of Software Engineering and Its Applications 8(2), 287–296, 2014

[16] Zhang, X., Wu, N., Yan, G., et al.: Hardware Implementation of Compact AES S-box. IAENG International Journal of Computer Science 42(2), 2015

[17] Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684-5.

[18] R. Buyya, C. Yeo, S. Venugopal, J. Broberg & I. Brandic, 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems. Journal of Future Generation Computer Science. vol. 25 no. 6 pp. 599-616

[19]] Y. Cao, C. Chen, F. Guo, D. Jiang, Y. Lin, B. Ooi, H.Vo, S. Wu, Q. Xu, ES2: A Cloud Data Storage System for Supporting Both OLTP and OLAP, Accessed on 24 May 2017

[20] L. Yao, J. Lu, J. Liu, D. Wang, and B. Meng, "A Secure and Efficient Distributed Storage Scheme SAONT-RS Based on an Improved AONT and Erasure Coding," IEEE Access, vol. 6, pp. 55 126–55 138, 2018