Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

www.ijarcsse.com

Research Paper

Available online at: www.ijarcsse.com

Analysis of Cloud Based Storage as a Services

Abhuday Tripathi
CS Department, PSIT
Kanpur, Uttar Pradesh, India

***Abstract*— Cloud computing has been growing in the recent year. Various institution and organizations are using it for diverse purpose. We can utilize it for software development, or replace our office infrastructure with those available on cloud on pay-as-you-use basis. These possibilities generate very good future for IT industry but there are few challenges that needs to be overcome. These challenges are different from those of current technologies. They come from diverse background like network security issues, legal issues, encryption technology challenges and privacy issues. Any user of cloud would expect all it's services to be reliable and safe from attacks. They should also meet SLA perfectly. Cloud based storage services is different from other services available. It is used for online storage of data**

In this paper we have analyzed the cloud computing based storage services and its components .We have tried to find out the benefits these services provide and challenges that they are facing. We have also analysed the recent development happening in this field and future trends in technology.

***Keywords*— cloud computing, data storage, network security, privacy, encryption**

I. INTRODUCTION

Cloud computing provides for large enterprise renting mechanism for storage, compute power, application over internet. It is often compared with electric metering system. This saves or reduces organization's IT expenditure. It also speeds up the development of project. It also raises the need for customizing business process of large organization to take advantage of cloud computing [1]. Cloud storage is internet based service to remotely manage, maintain or backup organizational data available from any place on the globe with devices having browser and internet connections. There are lot of organization providing cloud storage service over public cloud like IBM, Microsoft, and Google etc. As the volume of data generated on internet is exponentially rising so there arise needs for software architecture that can provide logically infinite data storage. It is often compared with existing data centre of large organization. Existing data centres are not scalable and need for storage is rising exponentially. So cloud storage system based on distributed system has came into existence like Big Tabel,Casandra,Amazon S3[2].The high availability ,security and low network latency of traditional data centres is matter of great concern for vendors of cloud based storage. An effective cloud storage system provides data security and protection, recovery, data lifecycle management, optimized storage solutions and they can be easily provisioned [3].

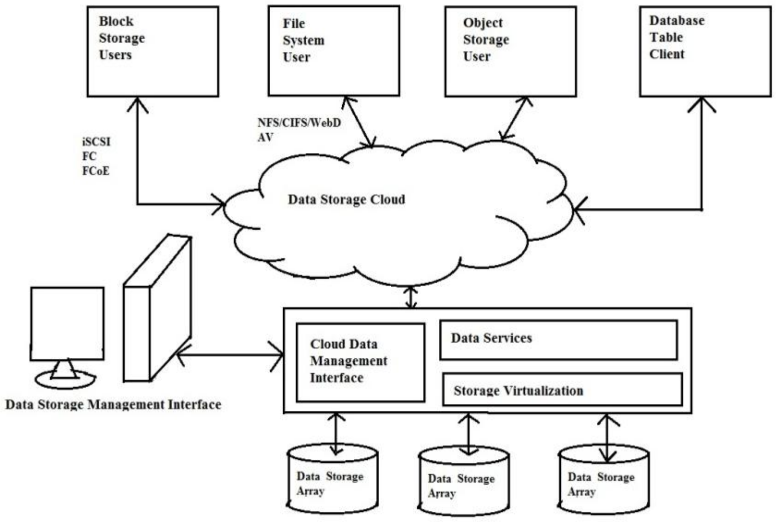

Fig.1 Components of cloud storage system

II. DEPLOYMENT MODEL FOR CLOUD STORAGE

Cloud based system can be easily understood as the composition of infrastructure and service. Here infrastructure mainly consists of hard disk, secondary storage which is virtualized before they are made available to user. There are various also services developed by the cloud service provider according to the need of their clients' .In [4] authors have suggested dividing the complete service into three categories. They are storage provider who take lot of cloud based storage service provider and provide service to general user. Cloud based service can be deployed in three different model. They are public cloud, private cloud and hybrid cloud .In [5] authors have found out why public cloud has certain limitations for business application. It cannot be said with certainty that public cloud is good for storage purpose. Some of the issues rose for business application like security, interoperability, data lock-in, absence of service level agreement, latency and network limits are also matter of great concern. Private cloud does mitigate some of the issues but not all.SLA should be well defined for cloud based service and it should be realistic. Network latency does cost a lot which compensates the benefit provided by cloud based services. Cloud user should find it easier to migrate their data from a cloud service provider's server to another's server. There should be industry standard available to make migration easier. Private cloud is always more secured than private cloud but the real advantage of public cloud is its pay-per-use-model which save the capital expenditure on IT infrastructure. Private cloud is not much different from data centers.Private cloud can be created by adding software automation and storage orchestration to storage infrastructure. This will provide on demand, self service and measured service to its users [6].

III. ADVANTAGES OF CLOUD BASED STORAGE

Cloud storage services are scalable, user friendly, saves bandwidth and accessible across the globe. They can provide zero infrastructure cost implementation of projects. Cloud storage services can be used for diverse purpose like sharing of data, backup, testing of project at reduced cost, database as a service and data analytics [7].Traditional data storage system includes NAS, SAN, DAS and data centre [8].

Table 1.Comparison of traditional data storage and cloud based data storage [9][10].

Aspects	Cloud based data storage	Traditional data storage
Distributed workforce	Cloud based data storage can be shared with geographically distributed users	Data owner has to manage the infrastructure distributed across the globe
Capital Expenditure	Capex is reduced as user only pay for services it is using.	Capex grows as the data volume grows. It does not contribute much to the profit.
Operational Expenditure	It reduces the need of IT staff and maintenance of infrastructure	Various kind of expenses like failure troubleshooting, capacity enhancement, Performance enhancement has to be taken care of by the user.
Disaster Recovery	CSP is responsible for the data recovery in case of disaster	User is responsible for handling disaster recovery.
Data Growth	User can easily scale up or down the quantity of storage it is using as the demand varies with time	User need to accommodate data into existing hardware or purchase new storage devices
Retention period	CSP provides reliable and long term storage of data.	User has to take care of hard disk failure or backup in case of tape drives
Power consumption	It is reduced	It increases with the growth in data volume.

IV. SHORTCOMING OF CCLOUD BASED STORAGE

Every organization's business process needs to be customized according to cloud storage's needs. The cost for using cloud storage is not clearly specified in SLA.In absence of internet connection cloud based storage service cannot be accessed. Security and privacy are also there. In [11] authors have classified the security for different service delivery models of cloud like IaaS,PaaS and SaaS.Such classifications can help us in developing different framework for different service delivery model. In [12][13] some of the vulnerabilities of cloud computing are mentioned. Same applies for cloud based storage service.

1. *Multitenancy*: Cloud service provider stores the data of multiple users on the same device. This is known as multitenancy.It can be implemented in various ways e.g., creating multiple partition on the disk or using vritualization.It should be the responsibility of the service provider to ensure that data of two user does not mix up with each other. Moreover the data should be permanently deleted and no one should not be able to recover the data from the disk allocated to any user after they have stopped using the service [**14**].

2. *Privacy and Security*: Data stored in local or personal server is always considered safer than data stored on others server. Cloud based service brings dependency on internet. Privacy and availability of data must be guaranteed by cloud service provider. In [15] authors have suggested dividing the data into two category i.e. sensitive and non sensitive data. Users must encrypt the sensitive data before they upload it on the cloud. Privacy of data also get violated due to illegal data mining by cloud service provider[16].Attack on application layer does exist for cloud based storage as it exists for any other services. Some of the possible attacks are XSS atack,cookie poisioning,hidden field manipulation,SQL injection,DDoS attacks, flooding attacks, network sniffing, port scanning,XML signature element wrapping attacks[17][18].Web 2.0 used for developing cloud based service involves lot of security threats like cross site scripting.DNS attacks on any website route its user to different location where user might store their sensitive data.

3. *Performance Unpredictability*: Performance issues related to data retrieval, storage, modification will always be compared before user moves to cloud based service from its local server. Overall performance may also decrease due to travelling of data from a network to another network or due to encryption and decryption of data. Virtualized server and processor sharing give degraded network performance [19].They can cause abnormal network delay.
4. *Portability and Interoperability*: Cloud based storage faces lock in issues where the user finds it difficult or impossible to move their data from one vendor to another vendor. This task may get more complicated due to different format of data storage, encryption or decryption of data. Deletion of data after it user has moved to different vendor must also be guaranteed.
5. *Vulnerability due to mobile cloud computing*: Lots of user access service with mobile phone or smart phone. This raises lot of challenges like network accessibility, network latency due to wireless connection, change in mobile phone, loss of confidentiality due to loss of mobile phone etc. It is easy for hackers to attack vendor's server with virus and malware from mobile system. Along with these threats security issues regarding data confidentiality, availability, integrity also exist [20].
6. *Data Confidentiality*: Cloud services are virtualized. There are several possible ways to compromise a virtual machine. and compromise the confidentiality of the data stored on them.Attackes can use cache details, system clock to compromise a virtual machine. There are several ways to prevent it like using symmetric key, access control list for easy resource. Symmetric key if shared with cloud service provider would prove it ineffective.
7. *Data Availability and Integrity*: Cloud service provider must guarantee availability and integrity of data stored on their server. There are cryptographic mechanisms for ensuring it. Uptime of service should be well mentioned in SLA.
8. *Infrastructure Level Compromise*: Attacker can use management interface to gain access into the cloud. Once successful entire service will fall into the hand of attacker. SOAP messages are mostly used in management interface. They can cause infrastructure compromise by giving root access to attacker.

V. SECURITY MEASURES

Encryption can be done at various layers. Users can opt for full disk encryption, virtual disk encryption or folder/file level encryption. Service provider must provide these facilities for protection against data theft due to multitenancy.[21].Google provides various kind of cloud services like Google Cloud storage, Google Cloud SQL,Google drive etc.Google employs various kind of security measures like x509 certificates for application's authentications' for accessing production environment. Google's employee work with their unique user id, follow Google's password policy. Google uses two factor authentication mechanism based on certificates and one time password generator in order to keep their management interface secure. Google performs automated/manual scanning of malware, network traffic monitoring for botnet attacks, uses authorized services and protocols, network firewall, routing all external packets to centralized server etc for the infrastructure security. Google replicates data at multiple geographically distributed data centres for ensuring data availability [22].AWS controls the physical component of their service. Everything else is control by the clients which includes encryption, identity and access management. So client is the real owner of data. Security process exists for multi tenancy issues[23].AWS provides HMAC ,TLS and RSA-1024 bit algorithms for further security but these algorithms does not guarantees its user privacy and integrity of data[24].In [25] authors have laid the need for new kind of encryption schemes e.g. proof of storage, searchable encryption scheme. Currently two variants of searchable encryption schemes have been developed. They are asymmetric and symmetric. Another encryption scheme of great use is identity based encryption schemes which can be used to enhance the privacy ensuring search [26]. In [27] authors have suggested the use of secure cryptographic processor. They have also designed protocols for ensuring privacy in the cloud based system. Trusted computing facility can help us in alleviating most of the problems of cloud .In [28] authors have proposed new scheme based on identity based encryption and attribute based encryption which provides fine grained access control over the data and full delegation.

VI. CONCLUSION

Undoubtedly if cloud computing based storage is properly implemented it will be the best form of cloud based services as we have seen above we are facing lot of challenges. We need to develop a proper access management system and identity management system which will ensure fine grained access control over the data stored on the cloud. It would also need proper key management system implemented by the cloud user. A lot of research is happening on new protocols like proof of storage, searching and indexing facility on encrypted data, public audit of data while maintaining its privacy, proof of deletion. They are still at infant stage and provide poor performance. Lot of work need to be done to make them practical and implementable. Audit mechanism can be used by service consumer to ensure that service provider is following SLA rigidly[29].We need to develop all these technologies keeping in mind the need of user of cloud based services. Obviously they will be very different from those used by non-cloud applications. Network performance can also be the reason behind poor service quality.This can happen due to geographical distance as well as virtualization.

ACKNOWLEDGMENT

I would like to express the deepest appreciation to Prof.Vineet Richariya, HOD CS Department, LNCT Bhopal without whom this paper would not have been possible. I would also like to thank my colleagues for helping when I was busy doing research on this paper. Lastly, but certainly not the least, I would like to thank my family for their support and their prayers for me which have been the driving force that enabled me finish this paper.

REFERENCES

[1] A.K.Hosseini,I.sommerville,I.Sriram.”Research challenges for enterprise cloud computing”.

[2] Q.Hi,Z.Li,Xiao Zhang.”Study on cloud storage system based on distributed storage system”..ICCIS 2010.

[3] ”Effective storage management and data protection for cloud computing”.IBM Software.Dec,2011.

[4] J.Chen,M.Lai,Y.Huang,G.Zhou.”The business model of cloud computing”..Cloud Computing 2010

[5] Paul Hoffman,Dan Woods.”Cloud computing :The limits of public cloud for business application”.

[6] A.Srivastava.”Storage as a service:SAN and NAS Refernce Architectures leveraging private cloud storage”.Avaialible at:” http://www.tcs.com/SiteCollectionDocuments/White-Papers/Storage-as-a-Service-SAN-NAS-Private-Cloud-0314-1.pdf”

[7] R.Aronika Paul Rajan ,S.Shanmugapriya.Evolution of Cloud Storage as Cloud Computing Infrastructure Service.IOSRJCE.1(1),pp-38-45. 2012,May-Jun.

[8] G.Somasundaram,A.Shrivastava.”Information Storage and management”.EMC Educational Services.Wiley Publishing,Inc.2009.

[9] B.Nisbet,L.Dubois.” The Benefits of Cloud-Based Backup: Addressing Business Continuity in a Distributed Work force”. .Sep,2011.Available at: https://mozy.co.uk/system/resources/W1siZiIsIjIwMTMvMTIvMTIvMTVfNDhfMzlfMTBfSURDX0J1c2luZXNzX0NvbnRpbnVpdHlfVUsucGRmIl1d/IDC_Business_Continuity_UK.pdf

[10] D.Csaplar.”The Proven Benefits of Backing-Up Data to the Cloud.” .Sep,2011.Avaialible at : http://research.aberdeen.com/1/ebooks/Proven-Benefits-of-Backing-Up-Data-to-the-Cloud.pdf

[11] Subashini, S. & Kavitha, V.,. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), p.1-11. 2010. Available at: http://www.sciencedirect.com/science/article/pii/S1084804510001281.

[12] R.Bhadauria,S.Sanyal.”Survey on security issues in cloud computing and associated mititgation technique”.

[13] Dr.Nashaat el-Khameesy,Hossam Abdel Rahma.”A proposed model for Enhancing Data Storage Security in Cloud Computing Systems”..JETCIS.Vol. 3,No. 6.June 2012

[14] Fiaidhi, Jinan, Irena Bojanova, J Zhang, and LJ Zhang. 2012. Enforcing multitenancy for cloud computing environments. *IT Professional*.

[15] Chen, D. & Zhao, H., 2012. Data Security and Privacy Protection Issues in Cloud Computing. In 2012 International Conference on Computer Science and Electronics Engineering. IEEE, pp. 647-651. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6187862.

[16] Chow, R. et al., 2009. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In Proceedings of the 2009 ACM workshop on Cloud computing security. pp. 85-90.

[17] S.Qaisar,K.F.Khwaja.”Cloud Computing:Network security Threats and countermeasures”IJOCRIB.Vol 3.No.9.Jan 2012.

[18] Shaikh, Farhan Bashir Fb, and Sajjad Haider. 2011. Security threats in cloud computing. 2011 International Conference for Internet Technology and Secured Transactions: 214-219. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6148380.

[19] Wang, G. & Ng, T.S.E. The impact of virtualization on network performance of Amazon EC2 Data Center. In Proceedings - IEEE INFOCOM.2010.

[20] G.Booth,A.Soknacki,A.Somayaji.”Cloud Security:Attacks and Current Defenses”.8th annual Symposium on Information And Assurance.June 4-5,2013.

[21] K.Scarfone,M.Souppaya,M.Sexton.”Guide to Storage Encryption Technologies for End User Devices”. Special Publication 800-111.NIST.November 2007.

[22] *”Google’s Approach to IT Security”.Avaialaible at* https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf.

[23] Garfinkel, S.L. An evaluation of amazon’s grid computing services: EC2, S3, and SQS. *Center for*, p.1-15.2007. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.172.2239\npapers2://publication/uuid/74E97C55-5666-4DAC-A25A-284BFB651A56.

[24] ”Amazon Web Services:Risk and Compliance”.November 2013.URL: *https://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf*

[25] K.Seny,L.Kristin .Cryptogrphic Cloud Storage.Available at: http://research.microsoft.com/en-us/people/klauter/cryptostoragerlcps.pdf

[26] Boneh, D. & Franklin, M. Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing, 32(3), p.586-615.2003.

[27] Itani, W., Kayssi, A. & Chehab, A. “Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures”. In 8th IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2009. pp. 711-716.

[28] Wang, G., & Liu, Q. Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services. Control, 735-737.2010. ACM Press. Retrieved from http://portal.acm.org/citation.cfm?id=1866307.1866414

[29] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proc. 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS ’07), pp. 1–6, 2007.