ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Survey on Secure Multicloud Storage Systems

Vidhya T. Gaikwad[1],S. M. Bansode[2]

M. Tech Student, Department of CSE, SGGSIE&T, Nanded, India[1]

Asst. Professor, Department of CSE, SGGSIE&T, Nanded, India[2]

ABSTRACT: Nowadays, storing and accessing data in multi-cloud storage system is being a common solution adopted by large organizations. Such adaptation would make organizations store their large amount of data in an efficient way without worrying about their storage limits. It provides them with a flexible and dynamic storage that can grow and shrink based on the current need for data storage, and they pay based that. Besides, it provide them with the gain of multiple services from different clouds. Hence, it is been a cost-effective solution especially when organizational data storage needs change dynamically through different time of the year. However, that solution comes with some challenges such as the lack of management and security issues. Security is one of the biggest challenges that face such platforms and it is defined in terms of data privacy, availability, confidentiality and access control enforcements. In this paper, we discuss some of the recent advances to provide multi-cloud security and the current adopted solutions in achieving security with their advantages and disadvantages**.**

KEYWORDS: Cloud computing, data privacy, data availability,Multi-cloud.

I. INTRODUCTION

Nowadays,cloud computing generate huge amount of data and that require to be store in an efficient and secure fashion. And today,cloud computing have taking a lot of research interest and industrial implementation.The reason why this is being so popular goes back to organizational needs and adaptation for cloud services including storage, platforms and other services that are offers by cloud providers as shown in figure 1.So Small, medium and even large organizations are not buying their own storage, they uses cloud services to store their data. The service is quit simple. It consists of a Cloud storage space assigned to a user for free or with reasonable fee.In addition, clouds can provide full functioning platforms to organizations allowing them to build their own specific platform and share it with others with worrying about their communication as soon as they are subscribed to the cloud.Hence cloud computing is being very popular today.

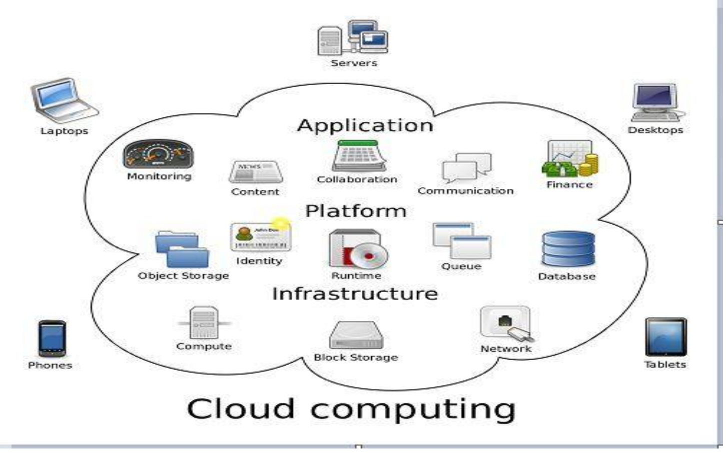

Figure 1: cloud computing

DOI: 10.15680/IJIRCCE.2016.0407134

Storing data over cloud represent good opportunity for cloud service provider to increase their revenues.The well-knownproviders include Dropbox,Google Drive,Copy,Amazon S3, and SkyDrive [10]. Despite the obvious advantages for the clients to use Cloud storage services to store any kind of data,several issues need to be addressed [10].For example,data privacy, availability, confidentiality, integrity.Recently, with the increase usage of clouds, organizations start adapting and subscribing to more than more cloud which introduces the concept of multi-cloud computing in both research and academic fields. For Example,would happen if an organization has alarge amount of data that can not be hosted on one small cloud provider so they mitigate to multiple cloud in order to support theirneeds.However, such strategies would come with a lot of challenges that includes guaranteeing organizational security aspects and the lack of management and control as the data is too separated.

Basic idea of multi cloud storage system is to use different service provider.Different from the traditional approach, each file is not stored as a whole in a single service provider, but it is divided into several pieces that are spread over different providers.

In this paper, we present multi-cloud storage security challenges and the current adopted solutions in achieving security with their advantages and disadvantages.

II. Security issues in cloud computing

- Data privacy: providers need to guarantee their data privacy in which unauthorized user don’t get access to confidential data.
- Data integrity: data integrity ensure that data cannot be modified by unauthorized user.
- Data availability: Providers need to guarantee availability in which users can access data at any time within their provider rules and policies.

III. multi-cloud

The term “multi-cloud” is similar to the term “intercloud” or “cloud of clouds” that were introduced by [1].Moving from single cloud to multi-clouds is reasonable and important for many reasons. the main purpose of moving to multi-clouds is to improve what was offered in single cloud by distributing the reliability, trust and the security among multiple cloud providers. Multi-cloud storage system is a distributed system where data have certain degree of redundancy and replicated among different clouds owned by different service provider.

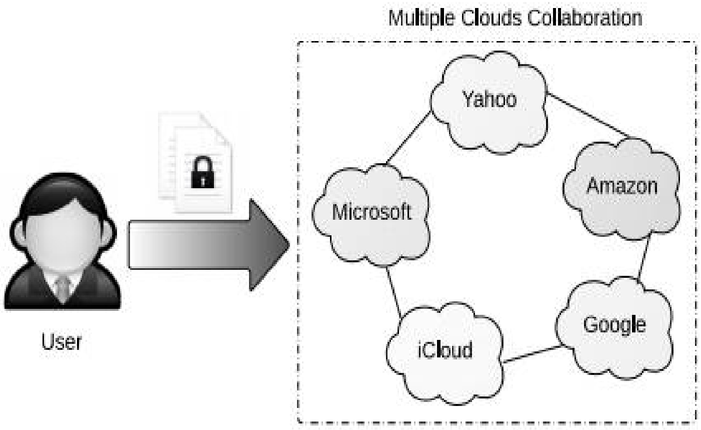

Figure 2: Simple Multi-Cloud Architecture

Multi-cloud storage system have several architectural view but they all have same component: clients, cloud storage servers, and a manger. A client is an entity which has massive data to be stored on multi cloud system .Cloud storage server is an entity which has significant storage space and computation resource to maintain the client’s data manager can be located inside the organization or outsources to a trusted entity. In this figure Manager is hosted inside the client and not shown in the figure 2.

DOI: 10.15680/IJIRCCE.2016.0407134

IV. EXISTING SOLUTIONS

A. Secure Cost-Effective Multi-Cloud Storage:

In this paper [5], author has proposed secure cost effective multi cloud storage model (SCMCS) in cloud computing which holds an economical distribution of data among the available service providers in the market to provide customers with data availability as well as secure storage.

In this model, customers divide its data among several service providers available in the market,based on his available budget.Also they provide decision for the customers to which SPs he must choose to access data, withrespect to data access quality of service offered by the SPs at the location of data retrieval. This not only rules out the possibility of a SP misusing the customer's data, breaching the privacy of data, but can easily ensure the data availability with a better quality of service.

B. Identity Based Distributed Data Provable Data Possession(ID-DPDP):

In this paper [7], author has proposed ID-DPDP protocol. ID-DPDP is a protocol that provide a secure and efficient integrity check based on data encryption.

The protocol consist of four module: setup, extract, tagGen and proof. In setup phase, input the security parameter k, it output the system public parameters the master public key and the master secret key. In extract phase ,Input the public parameters params, the master publickey mpk, the master secret key msk, and the identity ID of a client, it outputs the private key skIDthat corresponds to the client with the identity ID. The tagGenphase split the big chunk of data in to multiple blocks, store them in different clouds, generate a tag for each block and return back theBlock-tag pairs. The Proof algorithm would take a challenge and its answer and return back if the challenge passed successfully or no.

To access data, as shown in figure 3. Client first get its private key from extract algorithm, create block-tag pair from the tagGen algorithm and upload it to the combiner This reaches the verifier which sends challenges to the combiner that distribute the challenge among multiple clouds. Those clouds would reply back with their answers which is aggregated to the verifier again to ensure that the client have the access right.

Result showed that the algorithm has a limited computation power can be implemented on mobile, flexible and scalable due to its low computation and storage overhead .In terms of security, it can be achieved by verifying the information each time it is queried and fail the request if it failed the verification. Moreover, it shows a low communication overhead which results in less complexity and reduce the security risks resulting from eavesdropping communications. However, it could achieve only integrity and privacy of data and the process of how the combiner can be trusted or located is still not discusses.

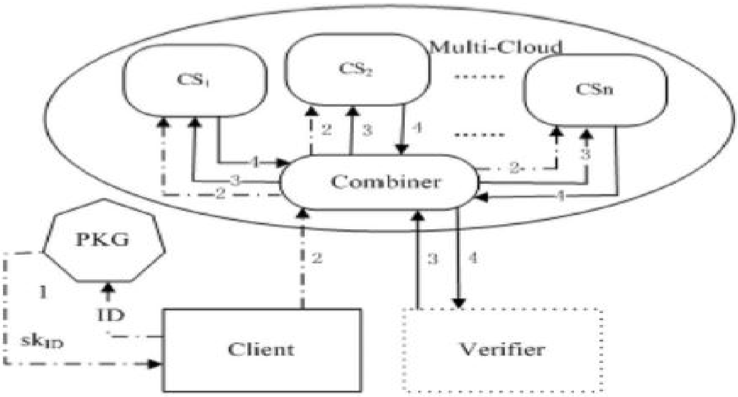

Figure 3: ID-DPDP system architecture

C. A Hybrid Cloud Approach For Secure Authorized Deduplication:

This scheme, as proposed in [8], explores the use of both private and public cloud to solve the problem of duplicates with different privileges access. The private cloud is used to store the keys for the files with specific privileges. In order to access a file, the user will need to have the key of that file and he need to be in a specific privilege. Hence, the private cloud is acting as aninterface between the user and the public cloud. Figure 4 highlights the protocol procedure in a simplified way In order to retrieve a file, the user sends the request to the public cloud which checks for the privilege and if the user has the read access. If it passes the check, the public cloud will send the data encrypted and the user can decrypt it using his own private key.

In such scheme, the user can assure that their data is stored securely and no unauthorized privilege can get access to data, which guarantees data privacy up to some level. However, such scheme comes with complex communication overhead during the storing process which adds delays and require key computation capabilities from clients, private clouds and public clouds.

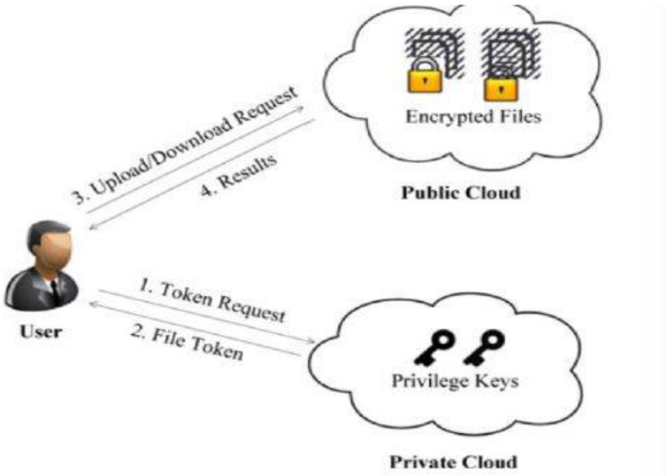

Figure 4: Secure Authorized Deduplication Architecture

D. Secure Big Data and Sharing Scheme for Cloud Tenants:

The authors in [9] provide a secure protocol to store big data that have both confidential and public privileges. The scheme protects the mapping of the confidential data into multiple clouds instead of protecting the data themselves. That is, as illustrated in Figure 5, when receiving some big data, they divide it into multiple parts and store them in multiple clouds. The location of those chunks will be held encrypted in the cloud indexing service such that no one other than authorized users can access them. When accessing a data, the client should send the request with the data encryption key and the cloud will collect the data from different part and send it backto the user. If the key was not matched then the cloudIndexing service cannot access the confidential data as the location will be encrypted. In this way, the data privacy can be guaranteed however data integrity and availability were not tackled. Besides, accessing the key, which is valid hacking strategy in some cases, can destroy the whole security purposes especially that all the location were encrypted with the same key.

DOI: 10.15680/IJIRCCE.2016.0407134

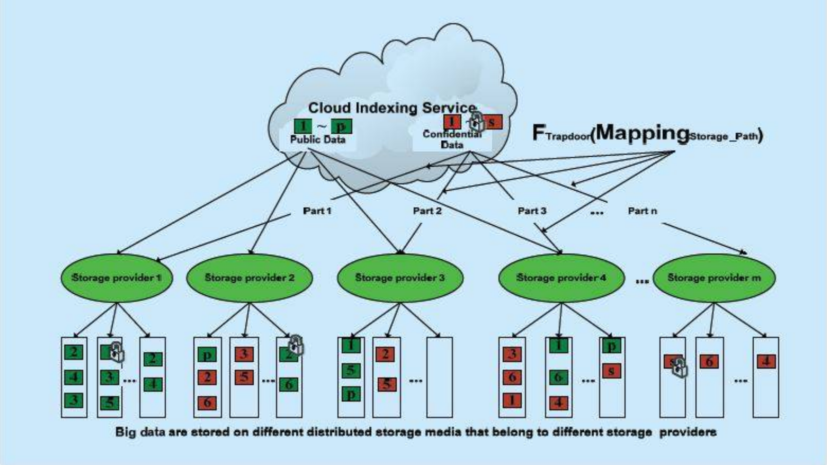

Figure 5: Cloud storage scheme for tenants big data

V. Comparing the Security Issues in Cloud Computing

TABLE I. Comparison based on security issues in cloud computing

Security Issues	Existing Multi Cloud Systems			
	SCMCS	ID-DPDP	Hybrid approach	Secure big data and sharing scheme
Data privacy	No	Yes	Yes	Yes
Data integrity	No	Yes	Yes	No
Data availability	Yes	No	No	No

VI. Conclusion and Future Work

In this paper, we study and analyze multi-cloud storage in cloud computing. Customers put their data into single cloud which is liable to vendor lock-in risk. In addition, the loss of service availability and data integrity are the major problems for the customer. This paper presentedsome recent advances and schemes to provide multi-cloud security and their comparison based on security issues. Distributed based approaches seems to be simple but provide less security than others. Hybrid based approaches were more realistically meeting organizational needs however they comes with private cloud costs.

References

1. M. Vukolic ,“The Byzantine empire in the intercloud, ACM SIGACT News”, 41 (2010), pp. 105-111.
2. J. Li, D. Lin, A. Squicciarini, J. Li, and C. Jia, “Towards privacy-preserving storage and retrieval in multiple clouds”, Cloud Computing, IEEE Transactions on, vol. PP, no. 99, pp. 1–1, 2015.
3. M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishnan, G.-J. Ahn, and E. Bertino, “Collaboration in multicloud computing environments: Framework and security issues”, Computer, vol. 46, no. 2, pp. 76–84, Feb 2013
4. J.-M. Bohli, N. Gruschka, M. Jensen, L. Iacono, and N. Marnau, “Security and privacy-enhancing multicloud architectures”, Dependable and Secure Computing, IEEE Transactions on, vol. 10, no. 4, pp. 212–224, July 2013.
5. Y. Singh, F. Kandah, and W. Zhang, “A secured cost-effective multi-cloud storage in cloud computing”, in Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, April 2011, pp. 619–624.

6. X. Li, H. Ma, F. Zhou, and X. Gui, “Service operator-aware trust scheme for resource matchmaking across multiple clouds”,Parallel and Distributed Systems, IEEE Transactions on, vol. 26, no. 5, pp. 1419–1429, May 2015.
7. H. Wang, “Identity-based distributed provable data possession in multi cloud storage”, Services Computing, IEEE Transactions on, vol. 8, no. 2, pp. 328–340, March 2015.
8. J. Li, Y. K. Li, X. Chen, P. Lee, and W. Lou, “A hybrid cloud approach for secure authorized deduplication”, Parallel and Distributed Systems, IEEE Transactions on, vol. 26, no. 5, pp. 1206–1216, May 2015.
9. C. Hongbing, R. Chunming, H. Kai, W. Weihong, and L. Yanyan, “Secure big data storage and sharing scheme for cloud tenants”, Communications, China, vol. 12, no. 6, pp. 106–115, June 2015.
10. Antonio Celesti n, Maria Fazio, Massimo Villari, Antonio Puliafito,’’ Adding long-term availability, obfuscation, and encryption to multi-cloud storage system.’’, in journal of network and computer Application 2014 Elsevier ltd.

BIOGRAPHY

Vidhya T. Gaikwadis student of Computer network and information security Department, Shri Guru Go bind Singh institute of engineering and technology, Nanded. She received Master of Technology (M.Tech) degree in 2016.from SRTMU, Nanded, MS, India. Her research interests are cloud security.