IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 3, March 2016

A Multi-Cloud Approach Towards Addressing Security Issues of Cloud: A Survey

Kumar M.V[1], Poornima A. S[2]

Assistant Professor, IS&E Department, Adichunchanagiri Institute of Technology, Chikmagalur, India [1]

Associate Professor, CS&E Department, Siddaganga Institute of Technology, Tumkur, India [2]

Abstract: Cloud offers resources to the users like hardware, software and allows users to access services from anywhere in the world at anytime through internet. Cloud also provides huge amount of space for the user to store their valuable data. Cloud users expect services from cloud service providers (CSP) in most of the time, so cloud providers should be always active. If a cloud service provider is failed due to some problem, then users can't access his/her data from cloud. This results in shifting the attention of the users from single cloud to multi-clouds. Even-though the cloud has many advantages, cloud users are still feeling insecure to use cloud. Security of the outsourced data to cloud is a major concern. This survey provides an in-sight on various multi-cloud security schemes which addresses some of the important security issues of cloud like integrity, confidentiality, service availability. The survey also provides the comparison of the schemes with respect to the issues they addressed.

Keywords: DNA Encryption, Trusted Third Party, CPDP, CSP, MCDB, VPC.

INTRODUCTION

Cloud computing is an internet-based computing model, in which resources, data and information are provided to users on demand. It helps users and enterprises by providing capabilities to store and process their data in cloud. National Institute of Standard Technology provides definition for the cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. network, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction" [3]. The usage of cloud leads to optimisation of resources.

The services provided by the cloud are classified based on the type of service delivery model as: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) [2]. In infrastructure as a service, users are provided with physical storage, processing, networking and other resources. Amazon EC2 provides this type of service. In platform as a service, users are provided with platforms like operating system, in which they can run their applications. Google App Engine, Microsoft AZURE provides this type of service. In software as a service, users are benefited with softwares to process their data. There are four deployment models identified in the cloud architecture: private cloud, public cloud, hybrid cloud, community cloud [1].

Although cloud service providers offer lot of benefits to the users, security is a major concern in cloud environment. Some of the major security factors which affect the cloud are data integrity, data confidentiality and service availability.

Data Integrity is one of the important issue in cloud. The data stored in cloud may be damaged or altered during transition operations or by some unauthorized users. When data is moved in a network, the receiver requires a verification to ensure that data has not been modified. In cloud, users store their data and will not possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed.

Data confidentiality is all about maintaining the secrecy of the outsourced data, so that unauthorized user should not be able to know about our data which is resided in cloud.

Service availability is all about providing data to the legitimate cloud user whenever he/she wants even when the cloud service provider is failed due to some unavoidable circumstances.

The rest of the paper is organized as follows. In section 2, some of the related works which address the security issues in multi-cloud are discussed. In section 3, a comparative study of different multi-cloud schemes have be done. Finally, section 4 concludes the survey.

RELATED WORK

This section discusses some of the work done in multi-cloud environment for addressing the security issues. Single-clouds are gaining less popularity among the cloud users due to the problems like service availability failure, malicious insider attacks and so on.

Ingale vinod bhimrao et.al [4] addressed an efficient Cooperative Provable Data Possession (CPDP) scheme for ensuring the integrity of outsourced data. There are two techniques used for constructing CPDP, they are hash index hierarchy and homomorphic verifiable response. In hash index hierarchy, the responses of the clients from multiple Cloud Service Providers are combined into a single response. Homomorphic verifiable response which

supports distributed cloud storage and implements a collision resistant hash function. Trusted Third party (TTP) generates and stores the public key and is used to store verification parameters.

Cloud user or data owners uses the secret key to process a file which is converted into set of data blocks and generates a set of public verification information which is stored in Trusted Third Party and transmits the file and verification tags to Cloud Service Providers. Then clients will issue a challenge for one CSP to check the integrity. Cooperative PDP is used to verify the integrity and availability of clients data stored in all Cloud service Providers.

There exist a small amount of computational and communication overhead when large files are considered. There is still a challenging problem in generating verification tags for variable sized data blocks.

M. Muhil, Hemanth Krishna et.al[5] applied shamir's secret sharing scheme for securing outsourced data in multi-cloud. This paper aims at providing a secure way for storing data to cloud and reducing the risk of data intrusion using shamir's secret sharing algorithm. Replication of data in several cloud is one advantage of multi cloud. So, when one cloud structure is under an attack, another cloud will provide the data. Thus the availability of data is not affected in this type of cloud. To secure the data in multi-cloud, data is encrypted and stored in more than one cloud.

The objective of the secret sharing algorithm is to divide the data into n pieces. Retrieving any k or more data pieces makes data easily computable but retrieving k-1 or less data pieces will makes the data undetermined and can't be useable.

Jens-Matthias Bohli et.al[6] addressed different multi-cloud architectures for security as well as enhancing of the privacy of the outsourced data. The idea of using multiple distinct clouds is to reduce the risks of malicious data manipulation, disclosure, and process tampering. Here different architectural models are used to distribute the resources to multi-cloud. Replication of application- In this model copy of the application will be distributed among multiple clouds and receive the result of operation performed in these multi-clouds. This enables the integrity of the data, but it doesn't guarantees the maintenance of confidentiality of the data. Partition of application system into tiers- this model allows us to separate the logic from data which helps in protecting data from leakage.

Partition of application logic into fragments and partition of application data into fragments - in these models distribution of the application as well as data into multiple clouds will be done by dividing them. Here cloud providers could able to know what information is stored in them. This helps in maintaining the confidentiality of the application. Homomorphic encryption technique is used to encrypt the data with public key and then upload cipher text to the cloud. The four major multi-cloud architectures has some weaknesses in terms of security guarantee, in terms of feasibility. Combining of these multi-cloud approaches would provide better result in terms of security.

Mohammed A. AlZain, Ben Soh et. al [7] proposed a multi-cloud databased model (MCDB) which is based on multi-cloud service providers and secret sharing algorithm. This model allows users to store different types of data and also permits them to execute different queries. MCDB model does not preserve security by single cloud but security and privacy of data will be preserved by applying multi shares technique on multi-cloud providers. It avoids the negative effects of single cloud, reduces the security risks from malicious insider in cloud computing environment.

MCDB preserves security and privacy of user's data by replicating data among several clouds and by using the secret sharing approach. The secret sharing algorithm is applied on the stored data in the multiple cloud providers. If the intruder or malicious insider wants to know the hidden information inside the cloud, they should retrieve at least three values from three different cloud service providers to be able to know the real value which has been converted and hidden before it stored at the multi clouds providers. If there are 3 shares stored in 3 cloud providers, knowledge of the value of 2 shares or less makes the secret un-constructible whereas the knowledge of the value of more than two shares will enable the value to be reconstruct. Thus MCDB addresses the data integrity issue.

MCDB replicates the data into three different cloud providers and hackers need to retrieve all the information from these cloud providers. If the hacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider. Hence, replicating data into multi-clouds by using a multi share technique reduces the risk of data intrusion.

Here static data is considered whose size is fixed and the cost of storing data increases with increase in number of shares. The data retrieval time also increases with increase in number of shares.

M. Sulochana et.al[8] proposed the concept of integrating distinct clouds to provide integrity and confidentiality for the user data. Administrator who resides in the private cloud will authenticate the user and allows only authorised user to access cloud resources. Cloud A user sends request to administrator to access Cloud B by entering his login credentials. Administrator will authenticate the cloud user A and allows him to access resource of cloud B.

The data uploaded by cloud user A to cloud B will be received by the administrator first. This data is encrypted using RSA algorithm. The encrypted data is further segmented and stored into different locations of the cloud B by the administrator. Here administrator will also perform de-segmentation and decryption when a request for data download takes place. This model ensures

integrity and confidentiality of the data as well as reduces the risk of data leakage.

All the security level activities are performed by the administrator. But, if the administrator is get compromised then even unauthorised user can also access to the cloud easily.

Richa H. Ranalkar et. al[9] have reviewed the concept of DNA encryption to secure the outsourced data in multi-clouds. DNA encryption is applied using two rules, base pairing rules and complementary rules. The generated cipher-text is then embedded into the DNA reference sequence for data hiding. According to biological terms, purine adenine (A) is always paired with pyrimidine thymine (T) and pyrimidine cytosine (C) is always paired with purine guanine (G). For computation purpose, G can be synthesised to T,A or C i.e combining all the base pairing rules we get 4x3x2x1=24. The probability of correct guess by attacker would be 1/24. Binary coding rule will convert binary data to DNA considering G=00, A=01, T=10 and C=11. Each user will be assigned with four character user-id like "TAGC" and system will generate the shift-key range from one to sixteen at random. System can generate 16^{16} combinations, as sixteen combinations can be shifted based on the key, i.e. generating more than 163 million unique DNA reference sequences.

Sayali S. Satav et. al[10] have addressed the security of the outsourced in multi-cloud using digital signatures. Digital signatures uses asymmetric cryptography. When messages sent through an in-secure channel, digital signature gives the receiver a reason to believe that the message was sent by the claimed sender. Blowfish technique helps to encrypt the data and RSA works on these encrypted data and generate the public key and private key. Public key will be generated for every file and Private key helps to generate the digital signature which is required for downloading. This Digital Signature will be accessed by user via mail. It also provides a better storage and security technique over Cloud architecture. By using RSA and digital signature security and privacy of the outsourced data can be enhanced, but less importance is given towards maintaining the service availability from cloud.

Yongdong Wu et.al[11] proposed a virtual private cloud (VPC) based on gateways which enables the users of each private cloud to access other private cloud securely. The VPC enables each user to perform authentication in its own cloud so as to obtain access to peer clouds. It provides a secure channel for users in the virtual cloud to communicate with each other via a third-party platform. Each enterprise has its own private cloud. In order to complete a task, several enterprises will form a collaborative cloud so that they can share resources. For accessing resources which are within a cloud may require any older authentication mechanism. For accessing resources which are in different clouds, gateway will authorise the user request on-behalf of the user. The VPC will translate the user request and send it to the collaborative cloud, because every cloud will have different access control schemes.

The VPC gateway builds a secure channel for users in collaborative cloud. When two users want to communicate with each other via a third-party platform the virtual cloud will build its own protection, as the third-party platform may provide no protection at all. To guarantee the security level defined by the enterprises, the VPC gateways should ensure end-to-end security. Both gateways should create a secure channel for any information exchange between them. After each user authenticates himself/herself to the third-party platform as usual, the gateway will encrypt all outgoing messages and decrypt all incoming messages. Authentication among VPC gateways across the collaborative cloud uses the Station-to-Station (STS) mutual authentication and key exchange protocol based on Public Key Infrastructure.
An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

COMPARISION

This section provides the comparison of some of the works which were carried out in the field of multi-cloud with respect to the security aspects which are supported by them. The security aspects that the cloud user expects the cloud to support are listed below [12]:

Data Integrity:- The stored data in the cloud may suffer from enormous damage occurring during the transition operations from or to the cloud storage provider. The risk of attacks from both inside and outside the cloud provider exists.

Data confidentiality:- The data should be kept secured and should not be exposed to anyone at any cost. The users do not want their confidential data to be disclosed to any service provider.

Service Availability:- It is one of the major security concern in cloud. Data stored in cloud and services should available to the user at anytime they wanted.

Intrusion Avoidance:- It is another security risk that may occur in a cloud provider. If any intruder can gain access to the account password, then he/she will be able to do any kind of unwanted changes to the account's private documents. Undesirable alteration of user data may commence due to intrusion.

Data Leakage Avoidance:- Unauthorised transfer of data from cloud will results in loss of valuable information of the user.

In paper [4], integrity and availability is achieved through Cooperative Provable Data Possession technique which is built using hash index hierarchy and homomorphic verifiable response. But it doesn't supports confidentiality, data intrusion and data leakage problem. In paper [5], shamir's secret sharing scheme is used for ensuring

integrity and also avoids data intrusion. But it doesn't support confidentiality, data leakage problem. In paper [6], four different multi-cloud architectures are discussed. In, replication of application architecture data integrity was achieved, but achieving confidentiality was not possible. In, partition of application system into tiers architecture data leakage can be avoided. In, partition of application logic into fragments and partition of application data into fragments architectures confidentiality of the data and availability was achieved.

In paper [7], multi-cloud database model was proposed to achieve integrity. The risk of data intrusion is avoided by using multi-share technique. In paper [8], integrity and confidentiality of the data is achieved through integrating distinct clouds. But service availability, risk of data intrusion is not achieved. In paper [9], security of the outsourced data is achieved through DNA encryption, but computation overhead may be more. In paper [10], integrity and confidentiality of the data is achieved through RSA and digital signature technique. But service availability, risk of intrusion and data leakage not addressed.

Table 1: Various Multi-cloud Schemes and the security aspects supported by them

Security Aspects Supported	[4]	[5]	[7]	[8]	[10]
Integrity	S	S	S	S	S
Confidentiality	NS	NS	NS	S	S
Intrusion Avoidance	NS	S	S	NS	NS
Data Leakage Avoidance	NS	NS	NS	NS	NS
Availability	S	S	NS	NS	NS

S -SUPPORTED, NS -NOT SUPPORTED

CONCLUSION

Data security is one the critical issue in cloud. We find many schemes in the literature which addresses different security aspects of the cloud. In this paper we compare few related works which are done based on the security aspects which are supported by them. The survey also provides an insight on some the shortcoming of the works which are carried out multi-cloud security. There is still less work done in the field of multi-cloud for enhancing the security of outsourced data. To conclude, there is still lot of scope in designing new schemes which could support all the security aspects in cloud, which draws attention of the users towards cloud storage.

REFERENCES

[1] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems 28, Pages 583-592, 2010.
[2] Pradeep Kumar Tiwari and Dr. Bharat Mishra, "Cloud computing security issues, challenges and solution", International Journal of Emerging Technology and Advance Engineering",Volume 2, Issue 8, 2012.
[3] Rajkumar Chalse, Ashwin Sleeker, Arun Katara, "A new technique of data integrity for analysis of the cloud computing Security", 5th International Conference on Computational Intelligence and Communication Networks, IEEE computer society, 2013.
[4] Ingale Vinod Bhimrao, Patil Pravin Ramchandra, "Data security of cooperative provable data in multi-cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, 2015.
[5] M. Muhil, U. Hemanth Krishna, R. Kishore Kumar, E. A. Mary Anita, "Securing Multi-cloud using secret sharing algorithm", Elsevier, 2nd International Symposium on Big Data and cloud computing, 2015.
[6] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo lacono and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE Transactions on Dependable and Secure Computing, Volume 10, Issue 4, 2013.
[7] Mohammed A. AlZain, Ben Soh, Eric Pardede, "MCBD: Using Multi-clouds to ensure security in cloud computing", Conference paper, 2011.
[8] M. Sulochana, Ojaswani Dubey, "Preserving data confidentiality using Multi-cloud architecture", 2nd international symposium on Big Data and cloud computing, Procedia Computer Science, pages 357-362, 2015.
[9] Richa H. Ranalkar, B.D. Phulpagar, "Review on multi-cloud DNA encryption model for cloud security", International Journal of Engineering Research and Applications, Volume 3, 2013, pp.1625-1628.
[10] Sayali S. Satav, Ganesh Prajapati, Sonali Dahiphale, Sadhana More, N. Bogiri, "Cloud computing security: From Single cloud to Multi-clouds using Digital Signature", International Journal of Advanced Research in Computer Engineering and Technology, Volume 4, Issue 4, 2015.
[11] Yongdong Wu, Vivy Suhendra, Huaqun Guo, "A Gateway based Access Control Scheme for Collaborative Clouds", 7th international conference on internet monitoring and protection, 2012.
[12] Satarupa Biswas, Abhishek Majumder, "A survey on data security in cloud computing: Issues and mitigation techniques", International Journal of Research in Engineering and Technology", Volume 2, Issue 2, 2013.