International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Replicating Data into Multi-Clouds by Using A Multi-Share Technique

[1]Harpinder Singh, [2]Sheetal Kalra

[1]Research scholar, GNDU, RC, Jalandhar(Punjab), India
harpinder2065@gmail.com

[2]Assistant Professor, GNDU, RC, Jalandhar(Punjab), India
sheetal.kalra@gmail.com

ABSTRACT

Cloud computing technology has increased rapidly in many organizations. It provides many benefits in low cost and accessibility of data to user. Ensuring the security of cloud is a main factor in the cloud computing environments. The customers do not want to lose their secret information, they often to store private data with cloud providers but these providers may be trusted or untrusted. Dealing with a single cloud provider is predicted to become less famous with customers due to risks of data intrusion, service availability failure and the possibilities of malicious insiders attack in the single cloud. The loss of service availability has cause many numbers of problems for a large number of customers. A movement towards multi-clouds (inter clouds) or cloud-of-clouds has emerged very recently. This manuscript focuses on security issues of single cloud system. Firstly, the paper survey the recent research of single and multi-clouds system and second it analysis the multi-cloud security techniques. This paper promotes the use of multi-clouds system due to reduce security risks.

Keywords- Data security; Single cloud; Multi-clouds;

I. INTRODUCTION

Cloud computing is the use of cloud resources (hardware and software) that are delivered as a service over a network (typically the Internet). A cloud service is generally used by the clients as and when needed, normally on the hourly basis. This "on-demand" or "pay as you go" approach makes the cloud service flexible. NIST further differentiates cloud as having five essential characteristics: On-Demand Self-Service, Broad Network Access, Measured Service (Pay-Per-Use), Resource Pooling (Multi-tenancy), Rapid Elasticity.

Cloud providers should address security and privacy issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failures and the possibility that there is malicious insider in the single cloud. There are some limitations of single cloud computing

1) Service availability failure
2) Possibilities of malicious insiders in the single cloud.
3) Cloud providers should address privacy and security issues as a matter of high and urgent priorities.

Cloud computing in its most righteous form can be called the next generation of computer technology. Cloud computing offers limitless flexibility, better reliability, enhanced collaboration, portability, unlimited storage but how secure is it after all. If the safety of data cannot be assured when it is stored in our private server how can we be sure of its safety over the cloud? Data stored in the cloud storage can be compromised or lost. So users have to come up with a way to secure those files in cloud storage. User can encrypt data

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

before storing them into the cloud, which sorts out the disclosure aspects. The main disadvantages of single cloud system are service availability failures and possibilities of malicious insider attack.

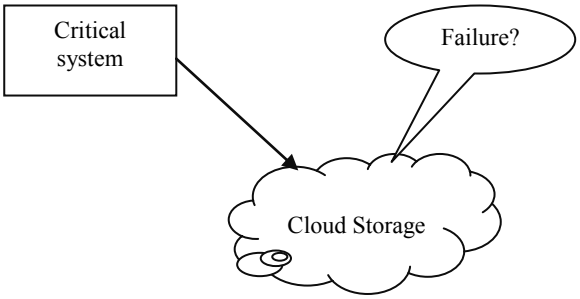

Fig.1 Service failure in cloud provider storage

Regarding loss of data or service availability risk, if user replicate the data into different cloud providers, it could argue that the data loss risk will be reduced in cloud computing. If one cloud provider service fails, user can still access the data live in other cloud providers. This has been discovered from this survey and user will explore dealing with different cloud provider interfaces and the network traffic between cloud providers. Multi-cloud strategy is the use of two or more cloud to minimize the risk of service availability failure, Loss and corruption of data, loss of privacy, vender lock-in and the possibility of malicious insiders in the single cloud system. The service unavailability can occur due to breakdown of hardware, software or system infrastructure cloud. A multi-clouds strategy can also be improve overall performance by avoiding vendor lock-in and using different infrastructures to meet the needs of diverse partners and customers. The cost of using multiple clouds will be higher than that of single clouds. Thus unless and until there is a design which can make use of multi-clouds without increasing cost, the implementation will be highly impractical.

Understanding the multi-clouds computing environment features provided to user.

1) The cloud computing security solution should meet the basic security and privacy requirements of any company deploying it.
2) Maintain an account of the privacy of the cloud and data security and applications that are deployed in cloud computing environment.
3) Ability to run custom application using service provider's resources.
4) Data Integrity.
5) Service Availability.

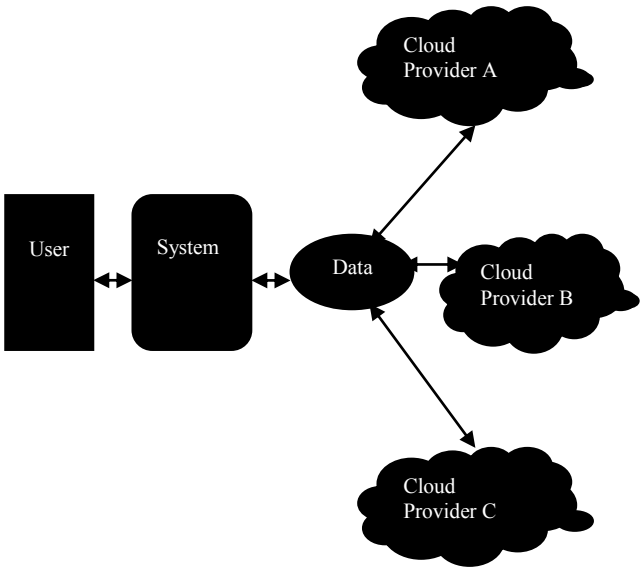

Fig.2 Data transmission to multi-clouds system

II. Security Issues of Single Cloud System

Security is most crucial aspect of everyday computing; this is very well applicable to cloud computing itself. There are many security concerns in cloud computing security. Keiko Hashizume [17] presented security issues of single cloud service models: SaaS, PaaS, and IaaS. As described in this paper, storage and networks are the biggest security concerns in Cloud Computing technology; a few security issues can be listed as follow:

A. Data Integrity

Data integrity is one of the most important issues related to cloud security. The data stored in the cloud storage may suffer from damage problem during transmission operations from or to the cloud storage. Any unintended changes in data as the result of a storage, retrieval or processing operations,

including malicious intents, unexpected hardware failures, and human error, is failure of the data integrity security. If the changes are the result of unauthorized access, it may also be a failure of data security. Example of data breaches occurred in 2009 in Google Doc, which triggered the Electronic Privacy Information Centre for FTC (Federal Trade Commission) to open an investigation into Google's Cloud Computing Services [1]. Another example of security risk to data integrity recently occurred in Amazon S3 server where users suffered problem from data corruption [2]. The data integrity risks are Sniffing/Spoofing virtual networks, MITM (Man-In-The-Middle) attacks etc.

B. Data Intrusion

An attack against cloud computing system can be silent, because if someone gains access to user account password, they will be able to access all the account's instances and resources of user account. Thus, stolen password allows the hacker erase all the information inside any virtual machine instance for stolen user account, modifies it, or even disables its services. Garfinkel [3], another security risks may occur with a cloud provider, such as the Amazon's cloud service, is hacked password or data intrusion. There multiple data intrusion attacks are: Data Leakage, Denial of Service, Account Hijacking, Data Scavenging, Malicious VM Creation, VM hopping,

C. Service Availability

Another major concern in cloud computing services is service availability. The loss of service availability is considered one of the main limitation of cloud computing. Amazon [4] mention in licensing agreement it is possible that the service might be unavailable from time to time to user. The user's web service may be terminating for any reason at any time if any user file breaks the cloud computing storage policy. In addition, if any damage occurs to web service and the service fails or errors, in this case there will be no charge to the Amazon Company for this failure or error. The loss of data has caused many problems for users, such as the problem that occurred in October 2009 when the contacts, photos and other data of many users of the Sidekick service in Microsoft server were lost for several days [5]. Bessani [6] use Byzantine fault-tolerant replication to store user data on several cloud provider's servers, so if one of the cloud provider's is damaged or failed, they are still able to retrieve data correctly from other cloud providers.

D. Confidentiality

Confidentiality of data is another security issue associated with cloud computing technology. The data should be kept secured and should not be exposed to anyone at any stage or any cost. The users do not want their confidential data to be disclosed to any other service provider or users. But it is not always possible to encrypt the data before storing it in cloud.

E. Non- Repudiation

Non-repudiation is a major concern for data security problems. It guarantees the transmission of message between parties and gives the assurance that someone cannot deny something. Non-repudiation is often used for signatures, digital contracts, and email messages. It ensures that a party cannot deny the genuineness of their signature on a documents or the sending of a message that they originated.

III. RELATED WORK

According to Tabakiet [8] described the way of responsibility for privacy and security in a cloud computing is shared between users and cloud service providers differ between delivery models. In software as a service, cloud providers are more responsible for the privacy and security of applications than the users. These responsibilities are more relevant to the public than the private cloud environment because the user need more strict or powerful security requirements in the public cloud. In platform as a service, users are responsible for taking care of applications that they are building and run on the platform,

while cloud provider are responsible for protecting user's applications from others. In infrastructure as a service, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the user's data.

Amazon web [7], their EC2 addresses security and privacy control in relation to physical, environmental, and virtualization security, whereas the users remain responsible for addressing security control of information technology system including the operating systems, applications and data.

Mohammed A. Alzain [9] purpose of this work is the recent research on single cloud and multi-clouds to address the security risks and its solutions. In this author have found that much more research has been done to ensure the security of single cloud and cloud storage whereas multi-clouds have received less attention in the ar ea of security. Authors support the migration to multi-clouds due to its ability to decrease security risks that affect the single cloud computing user.

Ristenpartet [10], in this paper claims that the levels of security issues in IaaS infrastructure service are different. This impact of security issues in the public cloud is greater than the impact in the private cloud model. For instance, any damage occurs to the security of physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud computing environment, the physical infrastructure is responsible for data processing and data storage can be affected by security risks. In addition, path for the transmitted data can also be affected, especially when the data is transmitted to many third-party infrastructure devices.

CERN (Institute, 2013) [11] according to CERN it defines an insider threat such as a malicious insider threat to an organization is a current or former employees, contractors, or other business partners who has or had authorized access to an organizations network system, or data and intentionally exceeded or misused that access in a manner that negatively affected the secrecy or confidentiality, integrity, or availability of the organizations information systems.

Bessani [8] use Byzantine fault-tolerant replication to store data on several cloud servers, so if one cloud providers is damaged, they are still able to retrieve data correctly from other data providers. Data encryption is considered the solution to address the problem of the loss of privacy. They argue that to protect the stored data from a malicious insider attack, users should encrypt data before it is stored in the cloud storage. The data will be accessed by distributed applications; the DepSky system stores the cryptographic keys in the cloud system by using the secret sharing encryption algorithm to hide the value of the keys from a malicious insider or other attacks.

According to Mohammed A. Alzain et al. [19], shifting from single cloud to multi-cloud is very important for ensuring the security of user's data. Authors suggested that, there are three main security factors of data (data integrity, data intrusion and service availability) that needs to be considered as the major concern for cloud computing. They have proposed a new model called Multi-clouds Database Model (MCDB). A technique named Shamir's secret sharing algorithm [18], which is based on polynomial interpolation has been incorporated in the scheme. According to the algorithm [18], if a data D is shared into n pieces, that D is easily reconstruct able from k pieces, but even complete knowledge of k-1 pieces reveals no information about D. The authors have suggested that Cloud Computing should not end with a single cloud system. In their work, they have compared Amazon cloud service which is single cloud with their proposed multi-clouds model. This model guarantees the security and privacy of data in multi-clouds using multi shares technique instead of single cloud. The data is replicated among several clouds by using secret sharing.

IV. DEPSKY MODEL

The Depsky system model is proposed model that contains three parts: readers, writers, and four cloud storage providers, where readers

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

and writers are the client's tasks. Bessani [8] explain the difference between readers and writers for cloud. Readers can fail arbitrarily whereas, writers only fail by crashing. For example, they can fail by crashing; they can fail from time to time and then display any behavior

The Byzantine protocols involve a set of cloud storage (n) where n = 3 f +1, and f is maximum number of clouds which could be faulty. In addition, any subset of (n – f) cloud storage creates byzantine quorum protocols.

A. BYZANTINE FAULT TOLERANCE

Any faults in software or hardware are known as Byzantine faults that usually related to inappropriate behavior and intrusion tolerance. In this, it also includes arbitrary and crash faults. More research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction. Although Byzantine fault tolerance (BFT) research has received a great deal of attentions, it still suffers from the limitations of practical adoption and remains peripheral in distributed systems. The relationship between BFT and cloud computing has been investigated, and many argues that in the last few years, it has been considered as one of the major roles of the distributed system. Furthermore, many describe BFT as being of only purely academic interest for a cloud computing service. This lack of interests in BFT is quite different to the level of interest shown in the mechanisms for tolerating crash faults and errors that are used in large-scale systems. Reasons for that reduce the adoption of BFT are, for example, difficulties in design, implementation, or understanding of BFT protocols. As mentioned, BFT protocols are not suitable for single clouds system. Vukolic [15] argues that one of the limitations of BFT for the inner-cloud is that BFT requires a high level of failure independence, as do all fault-tolerant protocols. If Byzantine failure occurs to a particular node into the cloud, it is reasonable to have a different operating system, different implementation, and different hardware to ensure such failures does not spread to other nodes in the same cloud mode. In addition, if an attack happens to a particular cloud, this may allow the attacker to hijack the particular inner-cloud infrastructure.

B. SHAMIR'S SECRET SHARING ALGORITHMS

Data stored in the cloud storage can be lost or compromised. So, user has to come up with a way to secure those files that store in the clouds. User can encrypt them before storing them in the cloud, which sorts out the disclosure aspects.

Encryption:

Step1: input- secretes key **k**, number of participant **n**.

Step2: select random values D1, D2…, Dn.

Step3: Generate polynomial string to share secrete into parts.

Step4: Secrete shared.

Decryption:

Step1: Generate polynomial string from secrete.

Step2: Add the n polynomial.

Our goal is to divide some data D into pieces D1, D2..., Dn in such a way that:

(i) The Knowledge of any k or more Di pieces to makes D easily computable.

(ii) The Knowledge of any k – 1 or fewer Di pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

This scheme is known as (k, n) threshold scheme. If k=n then all participants are required to reconstruct the secret original data.

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient for define a line, 3 points are sufficient for define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k points to define a polynomial of degree k-1.

We divide our secret into pieces by picking a random degree polynomial

$$q(x) = a_0 + a_1x + a_2x^2 + \cdots + {}_{a_{i-1}}\, x^{k-1}$$

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

In which a0= S, s1= q(1), s2=q(2),……, sn = q(n) and represent each share as a point $(x_i, q(x_i) = y_i)$.

V. Solution Analysis

Moving from single clouds to multi-clouds is reasonable and important for many reasons. Bowers [12] showed that over 80% of company organisations management fear security threats and loss of control of data and systems. HAIL (High Availability and Integrity Layer) is a protocol that controls the multiple clouds. HAIL is an example of distributed cryptographic systems that permits a set of servers to ensure that the client's stored data is retrievable and integral in cloud. HAIL provides software layer to address availability and integrity of the stored data into the interclouds system. Cachin [13] identify the two layers in the multicloud environment. The lower layer is the inner-cloud, while the second layer is the inter-cloud. In the inter-cloud, the BFT finds its place. It first summarizes the previous Byzantine protocols over the last three decades. The study present a design for inter-clouds storage (ICStore), which is a step closer than RACS and HAIL as dependable service in multiple clouds environment. Cachin develope theories and protocols to address the CIRC attributes (integrity, confidentiality, reliability and consistency) of the data stored in clouds. Abu-Libdeh [14] it assumes that to avoid vender lock-in, distributing a user's data among multiple clouds is a helpful solution on this. This replication also decreases the cost of switching provider and offers better fault tolerant system. The storage load will be spread among several providers as a result of the RACS proxy server. RACS (Redundant Array of Cloud Storage) for instance, utilizes RAID-like techniques that are normally used in disks and file systems, but for multiple cloud storage system. Bessani [6] present a virtual storage cloud computing system called Dep Sky system model which consists of a combination of different clouds to build a cloud-of-clouds or multi clouds. The Dep Sky system addresses the service availability and the confidentiality of data into their storage system by using multiple providers, combining Byzantine quorum system protocols, erasure codes and cryptographic secret sharing technique. Bessani [6] discuss some limitations of the HAIL protocol and RACS system when compared with DepSky cloud model. HAIL does not guarantee data confidentiality and data integrity, it needs code execution in their servers, and it does not deal with multiple versions of data. tThese limitations are not found in DepSky system, whereas the RACS system differs from the DepSky system in that it deals with economic failures, malicious insider and vendor lock-in and does not address the issue of cloud storage security problems. In addition, it also does not provide any mechanism to ensure data confidentiality or to provide updates of the stored data in cloud storage. Finally, the DepSky system described an experimental evaluation with several clouds, which is different from any other previous work on multi-clouds system. Vukolic [15] assumes that main purpose of moving to interclouds is to improve what was offered in single clouds by distributing reliability of data, trust, and security among multi-cloud providers. In addition, reliable distributed storage [16] which utilizes a subset of BFT techniques was suggested by Vukolic [15] to be used in multiple clouds system. A number of recent research studies in this area have built protocols for interclouds.

VI. Methodology and Future Work

Practical implementation of proposed work are has been done in this section. Proposed works implemented with NetBeans platform written in java. In this section it described all modules related to practical implementation. Net Beans is a software development platform written in Java. The NetBeans Platform allows applications to be developed from a set of modular software components called modules. Applications based on the NetBeans Platform, including the NetBeans integrated development environment (IDE), can be extended by third party developers.

The main aim of this work is provide a framework to supply a secure cloud database that will guarantee to prevent security risks and failure facing the cloud computing community. This framework will apply multiple clouds and the secret sharing algorithm of encryption to reduce the risk of data intrusion and the loss of service availability in the cloud storage and ensure the data integrity. In addition, data intrusion and data integrity, assume user want to distribute the data into three different cloud storage providers, and they are apply the secret sharing algorithm on the stored data in the cloud. An intruder needs to retrieve at least three values to be able to find out the real value that user want to hide from the intruder. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claims that even with full knowledge of (k – 1) clouds, the service provider will not have any knowledge of vs. (secret value). In other words, hackers need to retrieve the all information from the cloud to know the real value of the data in the cloud. If the attacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider (if k = 3) to know the secret which is the worst case. Hence, replicating data into multiple clouds by using a multi-share technique may reduce the risk of data intrusion, availability and increase data integrity. It will also decrease the risk of the Hyper-Visor being hacked and Byzantine fault-tolerant data being stolen from the cloud provider. Regarding service availability risk or loss of information, if user replicates the data into multiple cloud providers, they could argue that the data loss risk will be reduced. If one cloud provider fails, user can still access our data live in other cloud providers.

VII. CONCLUSION

There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. It is clear that although the use of cloud computing has rapidly increased but cloud computing security is still considered the major issues in the cloud computing environment. This paper focused on multi-cloud computing environments instead of single cloud for security reasons. The survey provided data integrity, data intrusion and service availability issues on single cloud system. The paper described the single to multi-cloud computing system and also analysis the multi-cloud computing security techniques which is helps in future for developing proposed technique.

ACKNOWLEDGMENT

I would like to thank Professor Sheetal kalra for helping me in this work and also all the other peoples who have encouraged me for this research.

REFERENCES

[1] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[2] Sun, http://blogs.sun.com /gbrunett/entry/ amazon_s3_silent_data_corruption

[3] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.

[4] Amazon, Amazon Web Services. Web services licensing agreement, October3, 2006.

[5] D. Sarno, "Microsoft says lost sidekick data will be restored to users", Los Angeles Times, October 2009.

[6] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

[7] G. Brunette and R. Mogull (eds), "Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009.

[8] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[9] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom,"Cloud Computing Security: From Single to Multi-Clouds" 45th Hawaii International Conference on System Sciences2012.

[10]T. Ristenpart, E. Tromer, H. Shacham and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", CCS'09: Proc. 16thACM Conf. On Computer and communications security, 2009, pp. 199-212.

[11]Institute, Software Engineering. The CERT Insider Threat Center. 2013. http://www.cert.org/insider_threat.

[12]K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. On Computer and communications security, 2009, pp. 187-198.

[13]C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

[14]H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[15]M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41, 2010, pp. 105-111.

[16]G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.

[17]Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez" An analysis of security issues for cloud computing", Springer. Journal of Internet Services and Applications 2013.

[18]A. Shamir, "How to share a secret", Communications of the ACM, Vol. 22, Issue 11, pp. 612-613, 1979.

[19]Mohammed A. Alzain, Ben Soh and Eric Pardede, "MCDB: Using Multi Clouds to ensure Security in Cloud Computing", Proc. of the 2011 IEEE 9th International Conference on Dependable, Autonomic & Secure Computing (DASC), pp. 784-791, 2011.