Enhanced Data Security from Single Clouds to Multi clouds

Ms. S. I. Bansod
Dept. of Computer Science &Engg, University of RGPV Bhopal, India
sarubansod@gmail.com

Abstract: The use of cloud computing has become viable in many organizations. The ease of data access and low investment has made cloud computing extremely popular. However, in un-trusted cloud environments, safety of sensitive data has become challenging. When considering the implementation of cloud computing services, data security threats are becoming a hindrance. Therefore, for better security solutions shifting from single cloud to multi cloud environments is a feasible option as with single cloud there is risk of the data being hacked, service availability failures and much more. This paper gives a survey on security merits making use of multi cloud environment and ways in which security can be enhanced choosing multi clouds. The paper proposes a useful way of managing the cloud storage and how it is ideal for most of the data attacks that often occur on single cloud environment. In this paper appropriate research analysis is done about the privacy concerns and data protection in cloud computing.

Keywords: cloud computing, cloud storage, multi cloud environment, cloud environments, data security, privacy concerns, cloud computing services.

I Introduction:

The security and privacy concerns need to be prioritize in cloud environments as cloud computing is the next generation paradigm in computation. In a cloud computing environment applications and resources need to be delivered on request over the internet. It is the concept of using remote services through a network with the help of several resources.

Single cloud environments are losing their popularity due to inefficacy of managing the challenges related to data security, service ability concerns and malicious insiders. It is the biggest obstacle when considering cloud computing services. There has been a shift from a single cloud to multi cloud environment. The paper will focus on the related issues with data availability and privacy concerns of a single cloud storage. Though cloud providers offer ample of benefits to their consumers, users online share a large amount of data online and they are aware of the potential loss of privacy.

There is innumerable amount of security challenges which are faced by the users like storing credit card details, medical records and personal information. This information need to be protected from malicious insiders and hackers. As the information is shared by third party, users of cloud computing will like to avoid untrustworthy cloud provider. Therefore, the shift from single cloud to multi cloud is examined and researched to deal with security issues successfully. The security issues are surveyed.

The primary objectives of this paper are:

- Improved accessibility for the data stored in cloud
- Proper security measurements and their implementation for confidential data in cloud
- Ways in which storage service reliability, data hacking, loss of information and downtime can be addressed.

The proposed cloud storage model DepSky with relevant details is explained to gain a detailed insight of it. The kinds of attacks and issues that the proposed model can withstand are stated in a precise manner.

Related Work (Literature Survey):

Cloud computing is considered as the new computing archetype which is highly cost effective and gives service on demand. It makes large scaled data storage and high performance computing easy. Thus, it has changed the way business are executing their operations and the merits are impeccable too. However, there are some challenges which businesses are facing by depending on Cloud Computing technology. There are many aspects of cloud computing and apart from the benefits, there are a few challenges which need to be addressed appropriately so the results can be promising.

The existing scenario of single cloud has many twists and turns that can hamper the efficacy of the business. The data shared on the internet connection needs to be secured else the business may have to face severe outcomes. The challenges and risks should be highlighted and resolved by the cloud provider. Therefore, migrating from single cloud to multi cloud can be helpful to avoid intrusion from hackers and malicious insiders.

The research is done on multi cloud models and how the migration is helpful to IT industries and other businesses. The different challenges can be met on multi cloud environment and how the proposed cloud storage model DepSky is able to address the risks and challenges which are faced on a single cloud.

1. Advantages of cloud services:

Some key benefits of using cloud services are listed below:

- Helps to select a virtual office and offers the flexibility of connecting to the business, anytime and anywhere.
- Cost of maintaining and managing the IT systems is lowered drastically. Need to purchase expensive systems and equipments for business is eliminated and the business can use the resources of cloud service provider.
- Migration of applications from one physical server to other becomes easy and the need to spend money on hardware, software or licensing fees is not required.
- It becomes easier for more work to be done in less time with less people
- When multiple redundant sites are used, reliability is improved that makes cloud computing ideal for disaster recovery and business continuity.
- Improves scalability as the business can scale up and down the operation and storage needs that swiftly matches the present situation and also allows flexibility to change when required.
- Maintenance is easier for cloud computing applications and the need of installing them to each user's computer is eliminated as it can be accessed from anywhere.
- The cloud services are on demand which the users can obtain, deploy or configure as per their need themselves.

2. Existing security concerns in single cloud models

Though cloud computing offers many advantages, there are some security concerns which have been highlighted in single cloud models like, compliance issues, data security and privacy, access management, loss of internal control, etc.

2.1 Data Security:

There is large number of risks involved in cloud computing environment even after so many merits. As data is stored in the cloud environment, there are multiple users on it and as the location of data is mobile, it can move easily from one place to other. The users on the cloud are unaware about the access log of their data along with the location of data. As the user is away from its information, it becomes more vulnerable and user's data security goes for a toss. As ample of people manage the cloud at one time, privacy cannot be guaranteed. Any amount of people can see the data.

2.2 Compliance Issues

The environment is challenging for cloud service providers as they need to comply with distinct regulations. Cloud is a combination of of several aspects like ample of people using same computing resource, , cross border locations and much more. Each aspect of cloud offers various set of regulations and rules which needs the service provider to follow it. The providers have to perform regular audits as user's data is stored away on cloud and most of the providers do not want to perform the audits as it is a costly affair for them.

2.3 Access Management:

As data is stored on different locations in cloud, it is mobile. The user of cloud may not know about the location of his data and as the cloud is multi tenant in nature the user may need to log on multiple times using different details. The details can be leaked out of the system and this poses risk. A robust and powerful identity as well as access management system needs to be in place for more cloud transfers.

2.4 Loss of Internal Control

The data in cloud is stored with the cloud service provider and the user of the data is generally away from it. As the data is not stored within the premises of the owner, the owner of the data may need to compromise with its security. This is a topmost challenge because the owner of the information feels unsafe and threatened about the security and use of the data as data is exposed to many people. Data is administered by different people and privacy concerns becomes a threat to users.

3. Migration to multi clouds

Migration from single to multi cloud environment ensures maximum security to the data of the user. Vukolic introduced the term multi clouds and it meant that cloud computing should not be dependent on a single cloud. Many recent researches have taken place to focus on multi cloud environment rather than depending on one cloud. The two layers are identified in the research in a multi cloud environment where the bottom layer is inner cloud where byzantine fault tolerance has its place. The second layer is inter-cloud.

Byzantine Fault Tolerance or BFT relates to intrusion tolerance and unacceptable behavior and also incudes crash faults. BFT has got a lot of attention and suffers from many limitations like practical adoption and BFT are not ideal for single clouds. According to Vukolic, BFT needs top level failure independence like other fault tolerant protocols. In case BFT failure happens on a node in the cloud, it is perfect to have a separate operating system, distinct implementation and unlike hardware that makes sure that such type of failure does not spread to other nodes in the same cloud. In case if there is an attack on any particular cloud,

Vukolic argues that one of the limitations of BFT for the inner-cloud [3] [4] is that BFT requires a high level of failure independence, as all fault-tolerant protocols. If Byzantine failure occurs to a particular node in the cloud, it is reasonable to have a different operating system, different implementation, and different hardware to ensure such failure does not spread to other nodes in the same cloud. In addition, if an attack happens to a particular cloud, this may allow the attacker to hijack the particular inner-cloud infrastructure only.

3.1 DepSky Algorithm

The DepSky system addresses the confidentiality and availability of data in the storage system with the help of multi cloud providers using BFT protocols and erasure codes. The architecture of DepSky is made of 4 clouds and each cloud make use of its own defined interface. The algorithm of DepSky is present in the client's machines like a software library that makes communication with every cloud. The 4 clouds are storage clouds so the need of code

execution is eliminated and the library allows reading and writing of the operations with the storage clouds.

3.2 Importance of DepSky:

A DepSky system helps to update stored information which is useful for this sort of application when the content that is distributed is dynamic and there are related security issues. It becomes easier for an organization to share and give detailed specifications about their business like inventory, price, etc. to the associates with better privacy, security and availability.

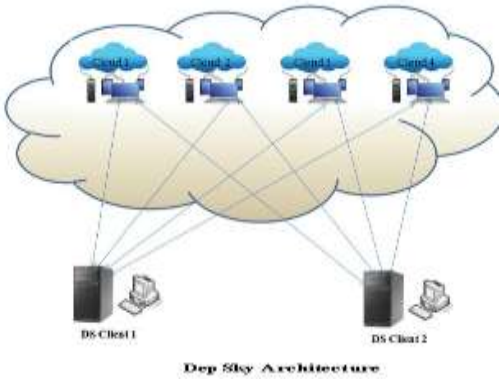
3.3 Benefits of The DepSky model

Firstly, the load on the servers can be reduced as every user can access the server to store just the fraction of file instead of complete file so the interaction time can be reduced with one given server instead of the four.

Secondly, the data sent or received is split and encrypted. Thus, the contents are secured. The data is sent on a secured SSL connection so there is no place for phishing or grabbing of the data.

Thirdly, the data is split and stored on all the four servers so in case one server is down, there is no downtime. The file is coded in such a way that the user can communicate with the remaining 3 to 4 servers and access the file.

Fourthly, the proposed model leaves no space for insider hacking as data files are split and distributed in 4 locations rather than a single location. In case a location is breached, the content is encrypted and enveloped with the help of compression algorithm so the data cannot be harmed. Moreover, in case of an attack there will be early warning signs and alters which is enforced by service provider's security.



Dep Sky Architecture

IJ

3.4 Multi Cloud Storage Analysis:

Shifting from a single cloud to multi cloud is effective and vital for several reasons. According to the conduced research (7) The single cloud service is subject to outage and as per the survey (6) it is seen that eighty percent of the IT professionals are insecure about the security threats and losing the control over data and systems. The main aim to shift towards inter clouds is to refine that is offered in single clouds by distributing trust, privacy and reliability among the different cloud providers. In conjunction, a dependable storage system which implements the BFT techniques is used for the multi-clouds.

4. FUTURE WORK

Here for implementation we have decided to develop two cloud projects:

1. Security Provider Cloud
2. Service Provider Cloud

Security Provider Cloud: This cloud will totally dedicate in providing security to the user. All the user that will be using services from cloud need to first login through this security provider cloud.
This cloud will first do registration of the user and provide username and password to the user. After it will verify the user and after security provider cloud approval user will be able to enter into service provider cloud.
Security provider cloud will always monitor the activity the user who is using services of the cloud. It can approve, reject or block the user according to the need.

Service Provider Cloud: Service provider work will only be providing services to the user, it will not look into security point since it will be handled by another cloud i.e. security provider cloud. After user is registered and approved by security provider cloud, it

will be connected to service provider cloud through web service and user and use services available to that cloud.

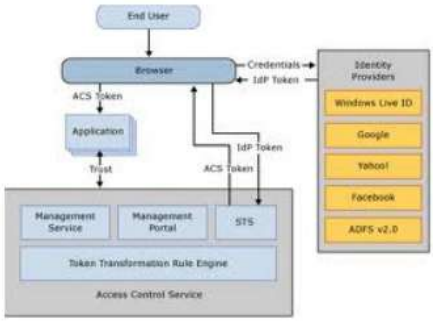


Fig 6: Access Control Framework

Cloud Computing facilitates storage of data at a remote site to maximize resource utilization. As a result, it is critical that this data be protected and only given to authorized individual. This essentially amounts to secure third party publication of data that is necessary for data outsourcing as well as external publications. We have developed techniques for third party publication of data in a secure manner. We assume that the data is represented as an XML document[7]. This is a valid assumption as many of the documents on the web are now represented as XML documents. First we discuss the access control framework proposed and then discuss secure third party publication. In the access control framework proposed security policy is specified depending on user roles and credentials. Users must possess the credentials to access XML documents. The credentials depend on their roles. For example, a professor has access to all of the details of students while a secretary only has access to administrative information. XML specifications are use d to specify the security policies[7]. Access is granted for an entire XML document or portions of the document. Under certain conditions, access control may be propagated down the XML tree.

For example, if access is granted to the root, it does not necessarily mean access is granted to all the children. One may grant access to the DTD's and not to the document instances. One may grant access to certain portions of the document. For example, a professor does not have access to the medical information of students while he has access to student grade and academic information.

5. CONCLUSION:

The paper has addressed the very important aspects of multi cloud environment that are beneficial to make a user feel secure about the data which is stored on the cloud. The issues related to availability of data, insider hackers, accessibility of data and security of contents of the data is addressed in a premium way too with the help of model. The . The proposed model algorithms are efficient to be used to enhance the overall efficiency of security and privacy concerns. This research gives a good support to users to shift from single cloud to public cloud as it has the ability to decrease security risks that may affect the cloud computing users.

6. ACKNOLDEGMENT:

This research was supported/partially supported by all saints colledge of engg. &technology bhopal. I would like to express my very great appreciation to mr Praveenkumar Kataria sir for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

REFERENCES:

[1] Desale Rutuja M, Jagtap Priya C, Labhade Swati P, Rokade Priyanka M, Prof. M. T. Jagtap , " Multi-cloud Data Security Using Shamir's Secrete Shearing", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper , Volume 5, Issue 1, January 2015

[2] Asst. Prof. Ingale, Vinod Bhimrao, Asst. Prof. Patil Pravin. Ramchandra, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper "Data Security of Cooperative Provable Data in Multi-Cloud", Volume 5, Issue 1, January 2015

[3] Mandar Kadam, Stewyn Chaudhary ,"Security Approach for Multi-Cloud Data Storage", International Journal of Computer Applications St. Francis Institute of Technology, Borivali (west) Mumbai, India September 2015

[4] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[5] Associate Professor, RajkumarB1, Balamurugan, K2 M.Tech , Dept of IT, K.S.R. College of Engineering, Tamilnadu, India, international journal Of innovative research in Computer and Communication Engineering "Service and Data Security for Multi Cloud Environment", Vol.2, Special Issue 1, March 2014.

[6] Yan Zhu, Member, IEEE, Hongxin Hu , Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, an Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 12, DECEMBER 2012.

[7] Mohammed A. AlZain, Ben Soh and Eric Pardede "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", Department of Computer Science and Computer Engineering, JOURNAL OF SOFTWARE, VOL. 8, NO. 5, MAY 2013

.