A DYNAMIC APPROACH TO CLOUD COMPUTING SECURITY OVER CLOUD OF CLOUDS

B. MURALI KRISHNA[1], MD. SHAKEEL AHMAD[2]

1, M.TECH Scholar, PBRVITS, Kavali
2, Associate Professor, PBRVITS, Kavali

ABSTRACT:

The convention of cloud computing has increased promptly in the society. Cloud computing have many benefits in terms of accessibility of data and low expenditure. A fundamental characteristic of the cloud services is that user's data are usually processed remotely in unknown machines that users do not operate. It can be transformed into a momentous roadblock to the wide adoption of cloud services. Make sure that the safety of cloud computing is a main factor in the environment of cloud computing, as users repeatedly store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is expected to become less accepted with customers due to risks of service accessibility collapse and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has come into view recently. The emergent popularity of cloud storage space services has show the way companies that handle critical data to think about using these services for their storage space requests. However the trustworthiness and safety measures of data stored in the cloud still remain main concerns. It is found that the research analysis into the use of multi-cloud providers to maintain security has acknowledged less thought from the research community has the use of single clouds. My effort aims to carry the use of multi-clouds due to its capability to decrease security risks that affect the cloud computing user.

Index Terms: ***Cloud computing, DepSky Architecture single cloud, multi-clouds, cloud storage, data integrity, data intrusion, service availability.***

1. INTRODUCTION

In this focuses on the issues related to the data security aspect of cloud computing. As data and information will be communicated with a third party, cloud computing users would like to avoid an untrusted cloud provider. Protecting personal and significant information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to multi-cloud surroundings is scrutinized and research related to security issues in single and multi-clouds in cloud computing is surveyed.

2. RELATED WORK

National Institute of Standards and Technology(NIST) describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources like networks, storage, servers, applications, services and that can be rapidly provisioned and released with minimal management effort or service provider interaction".

2.1 Cloud Computing Components

The cloud computing model had three delivery models, four deployment models and five characteristics. The five input distinctiveness of cloud computing are: location-independent resource pooling, on demand self service, rapid suppleness, premeditated service and extensive network admittance. These five characteristics correspond to the first layer in the cloud environment architecture.

ISSN: 2278 – 1323

Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Figure 1: Cloud Environment Architecture.

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking communications facilities, data storage space and computing services. It is the rescue of computer infrastructure as a service. A model of IaaS is the Amazon web service. In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. Cloud deployment models contain public, community, private and hybrid clouds. A cloud environment that is available for multi-tenants and is accessible to the public is called a public cloud. A private cloud is accessible for a particular group, even as a community cloud is modified for a specific group of customers. Hybrid cloud communications is a composition of two or more clouds. This model represents the third layer in the cloud environment architecture.

Fig.3: Cloud types

2.2 Cloud Service Providers Examples

In the commercial world, various computing needs are provided as a service. The service providers take care of the customer's requirements by, for illustration, maintaining software or purchasing luxurious hardware. For example, the service EC2, created by Amazon, offers customers with scalable servers. There are many features of cloud computing. First, cloud storages, such as AmazonS3, MicrosoftSkyDrive, or NirvanixCLoudNAS, authorize consumers to access online data. Second, it offers computation resources for users such as Amazon EC2. Third, Google Apps or versioning repositories for source code are examples of online collaboration tools

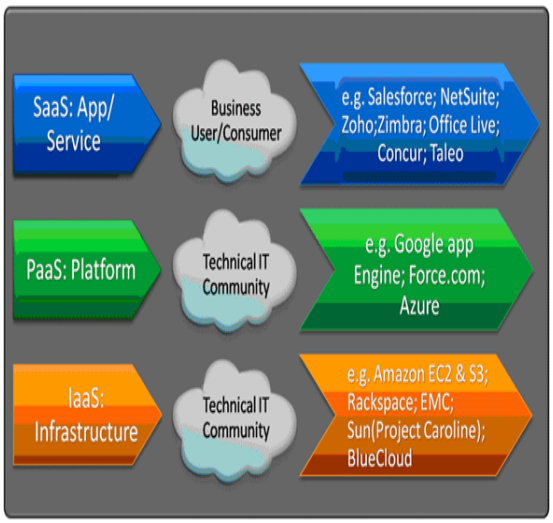

Fig 4: Cloud Computing Providers

ISSN: 2278 – 1323

3. SECURITY RISKS IN CLOUD COMPUTING

In multiple cloud service models, the security responsibility among users and providers is different. According to Amazon network, their EC2 addresses security control in relation to physical, and virtualization security, environmental, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

3.1. Data Integrity

It is not an easy task to securely maintain all essential data where it has the need in many applications for clients in cloud computing. To maintain our data in cloud computing, it may not be fully trustworthy because client doesn't have copy of all stored data. We have to begin new proposed system for this using our data reading protocol algorithm to check the integrity of data before and after the data insertion in cloud. Here the security of data earlier than and following is checked by client with the help of CSP using our "effective automatic data reading protocol from user as well as cloud level into the cloud" with truthfulness.

3.2. Data Intrusion:

The importance of data intrusion detection systems in a cloud computing atmosphere, We discover out how disturbance detection is performed on Software as a Service, Platform as a Service and communications as Service offerings, along with the accessible host, network and hypervisor based intrusion discovery options. Attacks on systems and data are a authenticity in the world we live in. Detecting and take action to those attacks has become the norm and is careful due diligence when it comes to security.

3.3. Service Availability

Service availability is most significant in the cloud computing security. Amazon previously mentions in its authorizing agreement that it is possible that the service might be unavailable from time to time. The user's web service may conclude for any reason at any time if any users files break the cloud storage policy. In accumulation, if any damage occurs to any Amazon web service and the service fails, in this casing there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

4. MULTI-CLOUDSCOMPUTING SECURITY

4.1. DepSky System: Multi-Clouds Model

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were launched by Vukolic. These terms propose that cloud computing must not end with a single cloud. Using their propose, a cloudy sky includes distinct colors and character of clouds which lead to different implementations and managerial domains. In the proposed system Bessani nearby a virtual storage space cloud system called DepSky which consists of a combination of dissimilar clouds to build a cloud-of-clouds. The DepSky system speak to the availability and the confidentiality of data in their storage system by using multi-cloud contributor, come together Byzantine quorum system protocols, cryptographic secret sharing and removal codes.

4.2. DepSky Architecture and Data Model

The DepSky architecture contains of four clouds and each cloud utilizes its have particular interface. The DepSky algorithm is real in the client's machines as a software library to communicate with each cloud. These four clouds are storage space clouds, so here no codes to be executed. The DepSky library gives permission reading and writing operations with the storage clouds. The uses of diverse clouds have need of the DEPSKY library to deal with the heterogeneity of the interfaces of each cloud provider. A feature that is particularly significant is the format of the data accepted by each cloud. The data model permits us to ignore these details when presenting the algorithms.

DepSky Data model:

As the DepSky system contract with a variety of cloud providers, the DepSky library agreements with

ISSN: 2278 – 1323

different cloud interface providers and as a result, the data format is accredited by each cloud. The DepSky data models having three generalization levels: the conceptual data unit, a generic data unit, and the information unit implementation.

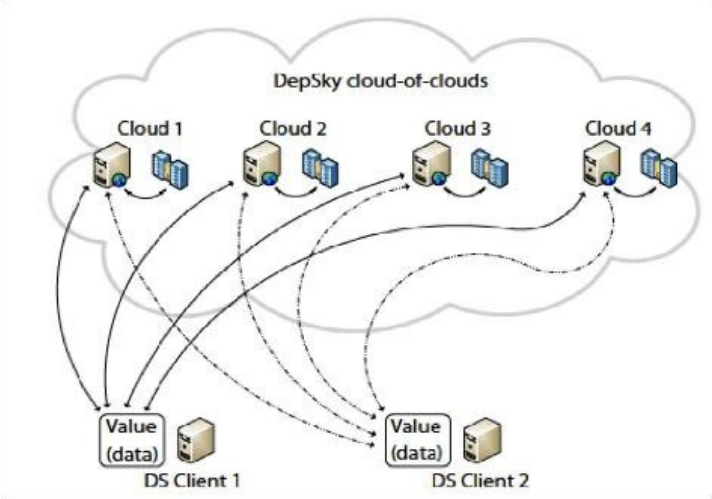

Fig.5: DepSky Architecture

The DEPSKY data model with its three abstraction levels. In the first (left), there is the conceptual data unit, which communicates to the basic storage object with which the algorithms work a register in distributed computing. A data unit has a exclusive name, a version number, verification data and the data stored on the data unit object. In the second level (middle), the theoretical data unit is implemented as a generic data unit in an abstract storage cloud. Each basic data unit, or container, holds two types of files: a signed metadata file and the files that store up the data. Metadata files hold the version number and the verification data, jointly with other information's that applications may demand. Notice that a data unit can store more than a few versions of the data, i.e., the container can hold several data files. The name of the metadata file is simply metadata, while the data files are called value<Version>, where <Version> is the version number of the data (e.g., value1, value2, etc.). Finally, in the third level (right) there is the data unit implementation, i.e., the container translated into the specific constructions supported by each cloud provider.

4. ANALYSIS OF MULTI-CLOUD RESEARCH

Moving from single clouds or inner-clouds to multi- clouds is sensible and important for many reasons showed that over 80% of company administration "fear security threats and loss of control of data and methods".. The trusty distributed storage space which utilizes a subset of BFT techniques was recommended by Vukolic to be used in multi-clouds. A number of present studies in this area have built protocols for inner clouds. RACS (Redundant Array of Cloud Storage) for example, utilizes RAID sample techniques that are normally used by disks and file systems, but for multiple cloud storage and assume that to avoid "seller lock-in", distributing a users data among several clouds is a cooperative solution. This reproduction also reduces the cost of switching providers and offers better fault tolerance. Therefore, the storage load will be extending among several providers as a result of the RACS proxy.

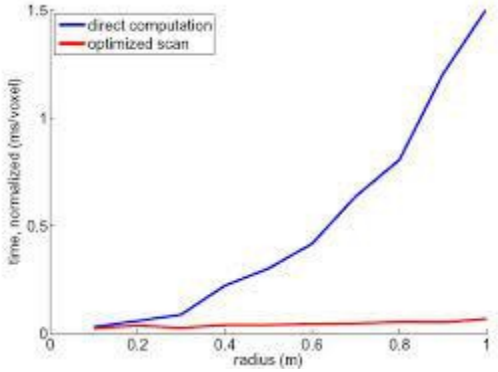

Fig: multi cloud analysis

4.1 Current Solutions of Security Risks

In order to decrease the risk in cloud storage, customers can make use of cryptographic methods to protect the stored data in the cloud. Hash function is a good solution for data integrity by keeping a short hash in local memory. In this manner, authentication of the server replies is done by recalculating the hash of the received data which is compared with the local stored data. If the amount of data is large, then a hash tree is the answer. Many storage system prototypes have implemented hash tree functions; claim that this is an active area in research on cryptographic methods for stored data authentication

ISSN: 2278 – 1323

5. CONCLUSION AND FUTURE WORK

In this present algorithms for performing addition, standard and scalar development with shares. We are currently developing a secure computation platform based on a simple secret sharing scheme than Shamir's. Cloud computing is currently the latest trend when it comes to online computing, it may help the enterprise and the end user by providing their needs, but the provider has to make convinced that they are precious and customer data is safe. We support the migration to multi clouds due to its ability to decrease security risks that is affect the cloud computing users

. The Further studies states to securely obtain the additional resources and availability of data is necessary. Security problems must be the first priority and thus switching of connection between the clouds must be with immediate reaction without any delay

6. REFERENCES

[1] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.

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

[4] Ittai Abraham, Gregory Chockler, Idit Keidar, and Dahlia Malkhi. Byzantine disk Paxos: optimal resilience with Byzantine shared memory. Distributed Computing, 18(5):387– 408, April 2006.

[5] Hussam Abu-Libdeh, Lonnie Princehouse, and Hakim Weatherspoon. RACS: A case for cloud storage diversity. Proc. of the 1st ACM Symposium on Cloud Computing, pages 229–240, June 2010.

[6] Hagit Attiya and Amir Bar-Or. Sharing memory with semi-Byzantine clients and faulty storage servers. In Proc. of the 22rd IEEE Symposium on Reliable Distributed Systems - SRDS 2003, pages 174–183, October 2003.

[7] Alysson N. Bessani, Eduardo P. Alchieri, Miguel Correia, and Joni S. Fraga. DepSpace: a Byzantine fault-tolerant coordination service. In Proc. of the 3rd ACM European Systems Conference – EuroSys'08, pages 163–176, April 2008.

[8] Kevin D. Bowers, Ari Juels, and Alina Oprea. HAIL: a high-availability and integrity layer for cloud storage. In Proc. of the 16th ACM Conference on Computer and Commu- nications Security - CCS'09, pages 187–198, 2009.

[9] Matthias Brantner, Daniela Florescu, David Graf, Donald Kossmann, and Tim Kraska. Building a database on S3. In Proc. of the 2008 ACM SIGMOD International Conference on Management of Data, pages 251–264, 2008.

ISSN: 2278 – 1323