Research Paper Engineering

Cloud Computing Security Using Secret Sharing Algorithm

*B.Arun **S.K.Prashanth

* M.Tech (C.S.E) VCE, Hyderabad India

** Prof. CSE, VCE, Hyderabad India

ABSTRACT

Cloud computing is a marketing term for technologies that provide computation software data access and storage services that do not require end-user knowledge. The use of cloud computing has increased rapidly in many organizations. General firms have already adopted the cloud computing and successfully applied to smart working for security and remote-services. The purpose of adopting cloud computing varies, yet the main purposes are to cut the cost, increase the work-efficiency, and ensure more security. "Single cloud" providers are predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. The use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Keywords : DEPSKY, virtualization, cloud providers

1. Introduction

Cloud computing, a newly developed operating paradigm, has been encouraged for enhancing the security as IT technology develops. It is a natural evolution of the wide spread adoption of virtualization, service – oriented architecture and utility computing .Cloud computing services uses in small and medium companies for various reasons, because these services provide fast access to their applications and reduce their infrastructure costs. There is use of multi-clouds in recent years. This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities want to avoid an un trusted cloud provider. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.

2. Cloud Computing Architecture

The two most significant components of cloud computing architecture

1. Front end
2. Back end

The Front end is the part seen by the client i.e the computer user. This includes the client's network and the applications used to access the cloud via a user interface such as a web browser. The Back end of the cloud computing architecture is the 'cloud' itself, comprising various computers servers and data storage devices.

3. How Cloud Computing Works?

The cloud consists of layers mostly the back-end layers and the front –end or user –end layers. The front-end layers are the ones you see and interact with when you access your email on Gmail for example. You are using software running on the front-end of a cloud. The same is true when you access your face book account. The Back-end consists of the hardware and software architecture that fuels the interface you see front end. Because the computers are set up to work together, the applications can take advantage of all that computing power as if they were running on one particular machine. Cloud computing also allows for a lot of flexibility, depending on the demand, you can increase how much of the cloud resources you use without the need for assigning specific hardware for the job or just reduce the amount of resources assigned to you when are not necessary. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.

3.1 Security

Security plays a central role in preventing service failures and cultivating trust in cloud computing. In particular, cloud service providers need to secure the virtual environment, which enables them to run services for multiple clients and offer separate services for different clients. In the context of virtualization, the key security issues include identity management, data leakage, access control, virtual machine protection, persistent client-data security, and the prevention of cross-VM side-channel attacks. Vendors and research communities are working to address these cloud-specific security concerns. The VM safe API provides VM security protection at the host level. To ensure integrity and authenticity, and to address access control in a cloud-enabled system, some have proposed using claim-based access control, a security assertion markup language, a security token service, and federated identity approaches. Undoubtedly, these low-level security concerns are important but to understand the issues related to consumer-level trust.

4. Dependable and secure storage in multiple clouds (DEPSKY):

The increasing maturity of cloud computing technology is leading many organizations to migrate their IT and/or adapting their IT solutions to operate completely or partially in the cloud. Even governments and companies that maintain critical infrastructures are adopting cloud computing as a way of reducing cost. Nevertheless, cloud computing has limitations related to security and privacy, which should be accounted for, especially in the context of critical applications. This paper presents DEPSKY, a dependable and secure storage system that leverages the benefits of cloud computing by using a combination of diverse commercial clouds to build a cloud-of-clouds.

In other words, DEPSKY is a virtual storage cloud, which is accessed by its users by invoking operations in several individual clouds. It addresses four important limitations of cloud computing for data storage in the following way:-

1. Loss of availability
2. Loss and Correction of data
3. Loss of privacy
4. Vendor lock-In

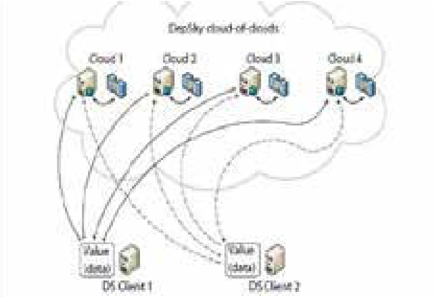

Fig 1: DEPSKY Architecture

5. Reduction of security risks

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud. Using a hash function is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses 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 solution Depsky uses a set of Byzantine quorum system protocols in order to implement the read and write operations in the system, so it needs only two communication round trips for each operation to deal with several clouds.

The use of several clouds needs a variety of locations, administration, design and implementation, which are the requirements of the Byzantine quorum systems protocols.

Executing codes in servers is not required in the DepSky system in contrast to other Byzantine protocols that need some code execution using these protocols, the DepSky system aims to deal with data confidentiality by decreasing the stored amount of data in each cloud.

6. Algorithm Review

A framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. This depends on a polynomial function technique which claims that even with full knowledge of (k – 1) clouds, the service provider will not have any knowledge of secret value (vs.).In other words; hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud.

Therefore, 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 (in the case where k = 3) to know the secret which is the worst case scenario.

Hence, replicating data into multi-clouds by using a multi-share technique may reduce the risk of data intrusion and increase data integrity. In other words, it will 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 data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers. This fact has been discovered from this survey and we will explore dealing with different cloud provider interfaces and the network traffic between cloud providers.

7. Conclusion

The purpose of this work is to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES

1. 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. 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. | 3. D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716. | 4. M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9. | 5. Amazon, Amazon Web Services. Web services licensing agreement, October3,2006. | 6. 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. | 7. 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. | 8. K. Birman, G. Chockler and R. Van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80. | 9. 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. |