Available online at www.sciencedirect.com

ScienceDirect

IERI Procedia 10 (2014) 112 – 118

Procedia IERI

www.elsevier.com/locate/procedia

2014 International Conference on Future Information Engineering

From Single to Multi-Clouds Computing Privacy and Fault Tolerance

Maha TEBAA*, Said EL HAJJI

University Mohammed V–Agdal, Faculty of Sciences,
Laboratory of Mathematics, Computing and Applications,
Rabat, Morocco

Abstract

Security issues of data hosted in a Cloud Computing provider remain hidden seen excessive marketing that led to a totally unrealistic view of cloud computing security. Although Cloud Computing has not yet reached the level of maturity expected by its customers, and that the problems of confidentiality, integrity, reliability and consistency (CIRC) are still open, the researchers in this field have already considered a future cloud strategy which aims : a better QoS, reliability and high availability, it is the Multi-Clouds, Cloud of Clouds or Interclouds.
This paper will present the security limitations in the single Cloud and the usefulness of adopting rather Multi-Clouds strategy to reduce security risks, through the use of DepSky which is a virtual storage system that ensures better availability and high confidentiality of data.

© 2014 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/3.0/).
Selection and peer review under responsibility of Information Engineering Research Institute

Keywords: Multi-Clouds Computing, Security, Privacy, DepSky, BFT, ICStore, HAIL, RACS ;

1. Introduction

Cloud computing is reshaping the IT domain, instead of unpacking computers and stack them in a machine room, the cloud can download virtually equipment and associated infrastructure, theconstruction of aDatacenter is now possible in some minutes with minimal technical knowledge and for a fraction of the purchase cost of a single server. Researches in the field of Multi-Clouds don't have much interest as the single

* Maha TEBAA. Tel.: +212-537-771-834; fax: +212-537-774-262.
E-mail address: maha.tebaa@gmail.com.

2212-6678 © 2014 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/3.0/).
Selection and peer review under responsibility of Information Engineering Research Institute
doi:10.1016/j.ieri.2014.09.099

Cloud. Although to date, little attention has been given to the distribution of cloud's risk, and managing multiple Clouds from a single technology platform, in the real world, by attaching your business to a supplier single is widely regarded as a bad strategy and unacceptable risks, and that philosophy applies to cloud provider with a single cloud, or even a single geographical area, as the case in EC2. To meet a variety of needs, including availability, business continuity and disaster recovery, it is important to use multi-Clouds strategies. Cloud providers themselves can fail, so for the greatest degree of protection, a company can engage in a Multi-Clouds strategy.

In this work we present the security limitations in the single cloud, and improvements to attributes (CIRC) through the use of a storage system in the multi-Clouds based on the consolidation of several clouds to put up the cloud of Clouds, to manage these various clouds, we use DepSky library in order to handle the heterogeneity of interfaces of each cloud provider. The DepSky system guarantees the availability and confidentiality of data by using multiple providers Clouds, by the association of "the algorithm of byzantine failures tolerance, secret sharing and erasure codes cryptographic". Then we compare DepSky with other storage mechanisms used on multi-Clouds, RACS, HAIL and ICStore that is currently under development and addresses the security aspects (CIRC) in a layered architecture.

2. Single Cloud Computing

Cloud computing is a new way of managing its infrastructure, applications and computer data over the Internet (VPN) by delegating administrative tasks of maintenance and supply of material resources to a third party (Cloud Computing provider), the only way to interact with data is an interface from their smartphone or computer, Cloud providers are essentially concerned by delivering services (PaaS, IaaS or SaaS), but ignore the main aspect which is the protection of privacy in the Cloud, and without any responsibility or obligation towards these customers, private data stored in plain cleartext in the virtual hard disk can be accessed by the provider itself or by other clients accessing the same disk.

2.1. Security limitations of the Single Cloud

Security issues of data stored in cloud are still the number one barrier to adoption of cloud computing for companies and government agencies. Security concerns are unavoidable for cloud computing to reach the level of maturity required, as the next generation of IT. Cloud services should ensure data integrity and provide privacy of the data stored in the cloud, but sometimes they lose control over the data stored in their data centers, as is the case in the following examples.

a) Data Integrity

Data integrity is one of the important issues related to Cloud security issues. The transmitted data between the client and cloud providers may be lost or corrupted, as shown in the examples bellow:

October 2009, a loss of all Sidekick users data (directories of contacts, calendars, photos) due to a server malfunction in Danger's data centers (Microsoft), after one year Microsoft has conceived that the majority of lost data cannot be recovered [2].

- January 2009, servers Ma.gnolia have suffered a total loss of data due to a complete failure; the loss of half a terabyte of data has made the process of recovery impossible, making the site essentially dead [3].

For more examples, refer to Cachinet and al [4].

b) Data Confidentiality and Privacy

Protect sensitive data such as bank details or documents healthcare should be among the priorities of cloud providers that are either internal (malicious administrators who work in the Cloud Provider) or external attacks. Various Cloud provider adopt various technology to resolve the problem of data privacy, but the virtualized nature of cloud make the traditional mechanism unstable for handling the privacy risks, and the use of the different encryption technique still limited. Garfinkel [5] gives an example of the loss of confidentiality such as the Amazon Cloud service. This example shows that just by knowing an Amazon

Download English Version:

https://daneshyari.com/en/article/554321

Download Persian Version:

https://daneshyari.com/article/554321

Daneshyari.com