Global Journals Inc.

Global Journal of Computer Science and Technology
Cloud and Distributed
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Challenge Token based Security for Hybrid Clouds

By Anukrati Dubey & Sandeep Sahu

*Shriram Institute of Technology, **India***

Abstract - Cloud has now become the essential part of the web technology and fast growth of cloud computing technique making it worth for the companies to invest in cloud. Growth of number of clouds is requiring inter cloud communication as concept of multi cloud or hybrid cloud is also spreading quickly. With this fast growth, more and more challenges are arising in the field of cloud computing. Various researchers are focusing on cloud oriented challenges and lots of research works are going on in this field. With emergence of cloud computing, the term "Hybrid Topology" or "Hybrid Deployment" is becoming more and more common. A "Hybrid Cloud" is group of clouds you join different cloud deployments into one connected cluster. Another area of research is to focus on communication between a cloud and non cloud computing system. Hybrid Cloud computing mainly deals with working of data centers where different software are installed with huge of growing data to provide information to the users of the system.

The techniques which can be used in hybrid cloud securities can be built around the encryption and decryption of data, key based security algorithms which are mainly oriented on authentication and authorization techniques as in wired and wireless networks. One such mechanism is to share the challenge text between the clouds before actual communication should start for authentication. The various works done in this area till date are oriented on other techniques of security between the two or more clouds in a hybrid cloud.

Keywords : cloud computing; hybrid cloud; challenge text; security.

GJCST-B Classification : C.1.4

Challenge Token based Security for Hybrid Clouds

Anukrati Dubey [α] & Sandeep Sahu [σ]

Abstract - Cloud has now become the essential part of the web technology and fast growth of cloud computing technique making it worth for the companies to invest in cloud. Growth of number of clouds is requiring inter cloud communication as concept of multi cloud or hybrid cloud is also spreading quickly. With this fast growth, more and more challenges are arising in the field of cloud computing. Various researchers are focusing on cloud oriented challenges and lots of research works are going on in this field. With emergence of cloud computing, the term "Hybrid Topology" or "Hybrid Deployment" is becoming more and more common. A "Hybrid Cloud" is group of clouds you join different cloud deployments into one connected cluster. Another area of research is to focus on communication between a cloud and non cloud computing system. Hybrid Cloud computing mainly deals with working of data centers where different software are installed with huge of growing data to provide information to the users of the system.

The techniques which can be used in hybrid cloud securities can be built around the encryption and decryption of data, key based security algorithms which are mainly oriented on authentication and authorization techniques as in wired and wireless networks. One such mechanism is to share the challenge text between the clouds before actual communication should start for authentication. The various works done in this area till date are oriented on other techniques of security between the two or more clouds in a hybrid cloud.

Keywords : cloud computing; hybrid cloud; challenge text; security;

I. Introduction

Cloud computing is becoming a buzz word in computer industry and everyone is looking to associate in one way or other with this brand new concept. Cloud computing is a very current topic and the term has gained a lot of traction being sported on advertisements all over the Internet from web space hosting providers, through data centers to virtualization software providers.

Special emphasis is put on the critical examination of each strategy as now more than ever in the face of the global economic crisis, companies face higher refinancing and investment costs and as any company thinking about adopting or moving to cloud computing technology would do in practice; short-to-medium term disadvantages of the technology have to be pragmatically and carefully weighted out against any hyped long- term potential efficiency achievements, be it strategic, technical or cost related. [1]

In order to understand the vision, goals and strategy behind cloud computing, two key concepts that form its foundations need to be explained first.

1. Autonomic Computing
2. Utility Computing

Autonomic computing, the term initially being introduced by IBM's Senior Vice President Paul Horn to the National Academy of Engineers at Harvard University in 2001, represents a research aim towards achieving self-managing computing systems, whose components integrate effortlessly.

Utility computing is the second key concept that one encounters in all cloud computing models. It is by no means a new concept as articulated in one form or another as early as the 1960s and implies that it is only natural that at some point computing power will be offered as a standardized service billed on actual usage with very limited or no upfront set-up charges.

a) *Cloud Computing – Definitions*

A scientific definition is proposed by the GRIDS Lab at the University of Melbourne:

"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers."

Berkeley's defines it as:

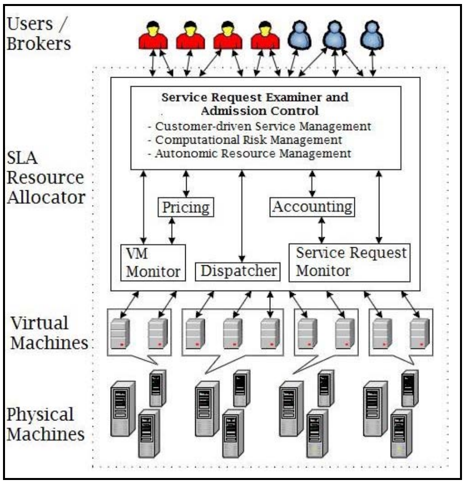
"Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services (Software as a Service - SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the public, we call it a Public Cloud; the service being sold is Utility Computing." [1]

Building blocks of cloud computing:

- Storage-as-a-Service
- Database-as-a-Service
- Information-as-a-Service
- Process-as-a-Service
- Application-as-a-Service

Author α : Student, Dept. of Computer Science & Engg, SRIT, Jabalpur, India. E-mail : anukrati_dubey@yahoo.com.com
Author σ : Asstt. Professor, Dept. of Computer Science & Engg, SRIT, Jabalpur, India. E-mail : s.sahu@iitg.ernet.in

- Integration-as-a-Service
- Security-as-a-Service
- Management/Governance-as-a-Service
- Testing-as-a-Service


Users / Brokers
Service Request Examiner and Admission Control
- Customer-driven Service Management
- Computational Risk Management
- Autonomic Resource Management
SLA Resource Allocator
Pricing
Accounting
VM Monitor
Dispatcher
Service Request Monitor
Virtual Machines
Physical Machines

b) Hybrid Cloud Computing

1. A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms.
2. A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid cloud is also referred to as hybrid IT.

3. *Challenges in Hybrid Cloud Computing*

Here are some challenges to consider when setting up hybrid clouds:

i. *On Demand Startup and Shutdown*

Your infrastructure must be able to start up and shutdown cloud nodes on demand. Usually you should have some policy implemented which listens to some of your application characteristics and reacts to them by starting or stopping cloud nodes. In simplest case, you can react to CPU utilization and start up new nodes if main cloud gets overloaded and stop nodes if it gets under loaded.

ii. *Cloud-based Node Discovery*

The main challenge in setting up regular discovery protocols on clouds is that IP Multicast is not enabled on most of the cloud vendors (including Amazon and GoGrid). Your node discovery protocol would have to work over TCP. However, you do not know the IP addresses of the new nodes started on the cloud either. To mitigate that, you should utilize some of the cloud storage infrastructure, like S3 or SimpleDB on Amazon, to store IP addresses of new nodes for automatic node detection.

3. *One-Directional Communication*

One of the challenges in big enterprises is opening up new ports in Firewalls for connectivity with clouds. Quite often you will only be allowed to make only outgoing connections to a cloud. Your middleware should support such cases. On top of that, sometimes you may run into scenario of disconnected clouds, where cloud A can talk to cloud B, and cloud B can talk to cloud C, however cloud A cannot talk to cloud C directly. Ideally in such case cloud A should be allowed to talk to cloud C through cloud B.

4. *Latency*

Communication between clouds may take longer than communication between nodes within the same cloud. Often, communication within the same cloud is significantly slower than communication within local data center. Your middleware layer should properly react to and handle such delays without breaking up the cluster into pieces.

5. *Reliability and Atomicity*

Many operations on the cloud are unreliable and non-transactional. For example, if you store something on Amazon S3 storage, there is no guarantee that another application can read the stored data right away. There is also no way to ensure that data is not overwritten or implement some sort of file locking. The only way to provide such functionality is at application or middleware layers.

II. Existing System

Paper [4] states that Cloud computing is setting off great changes in the IT industry. There are more and more researches on cloud computing. And this paper focuses on cloud computing too. At the beginning this paper describes the characteristics and definitions of cloud computing, and then introduced its services patterns (including SaaS, PaaS and IaaS) and deployment patterns (including public cloud, private cloud and hybrid cloud), at the end lists the cloud security challenges that cloud computing faces.

Security problems faced by the cloud system about in the following five aspects:

- First, face more security attacks: due to the vast amounts of user data stored in the cloud system, for attackers there has greater allure. If the attacker in some way successfully attack cloud systems, it will bring devastating disaster for both cloud providers and users.

- Second, virtualization technology: it not only brings cloud computing platform flexibly resources configured, but also brings new security challenges. There is a need to solve the problem that secure deployment of cloud platform based on the virtual machine architecture.
- Third, ensure continuity of the cloud platform services and high availability of user data and business: Amazon data center downtime event, Google's Gmail failing to use event and so on are associated with cloud computing availability. To a certain extent, the events above discourage the enthusiasm of the enterprise to use public cloud.
- Fourth, ensure the safety and privacy of user data: user data stored in the cloud system, for malicious attacks, the primary purpose is to get user privacy, and then to obtain economic benefits.
- Fifth, perfect the cloud standards: Interest-oriented IT development process leads to cloud standards exist everywhere. Many manufacturers have defined their own application standards and data formats, forcing the user deploying IT system and their own business in accordance with the framework set by different service provider [4].

With the advance of cloud computing, hybrid cloud that integrate private and public cloud is increasingly becoming an important research issue. Migrating cloud applications from a busy host to an idle host needs an efficient way to guarantee the performance in the geographical heterogeneous cloud environment [1].

From the studies of various research papers and works done by various researchers it has been found that following are the major areas of focus in the field of cloud computing:

1. Defining Architecture: on the basis of the application areas.
2. Security of communication over the cloud.
3. Integration of services on various layers.
4. Inclusion of Various network and communication devices being developed rapidly [1]

III. Proposed Algorithm

This work proposes a secured intra cloud communication mechanism in which it is being tried to keep the data more secured over the intra cloud communication using a challenge text based communication. Various Steps involved are as follows:

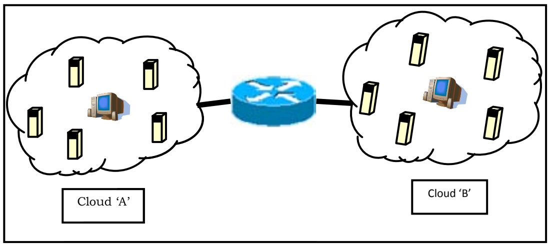
Step 1: Cloud 'A' has to communicate with Cloud 'B'. (Both 'A' and 'B' may be public, private or combination). Both have a trusted environment already created between them using SLA.

Step 2: Cloud 'A' sends a data request (DRQ) to Cloud 'B'.

Step 3: Cloud 'B' receives the DRQ and sends a challenge text (RID) encrypted using RSA algorithm, to Cloud 'A'.

Step 4: Cloud 'A' receives the RID and decrypts the same using its public key. The decrypted text (VID) is sent to the Cloud 'B'.

Step 5: Cloud 'B' if founds that the key is matching, it will send the encrypted data to Cloud 'A' as desired by the Cloud 'A'.



Step 6: Cloud 'B' if founds that the key is not matching, it will reject the request instantly.

DRQ- Data Request
RID-Reveal Identification
VID – Verify Identity

IV. Results

The algorithm is performing better in all situations such as a cloud is performing mal activities, cloud become malicious after a while or a cloud is not at all malicious.

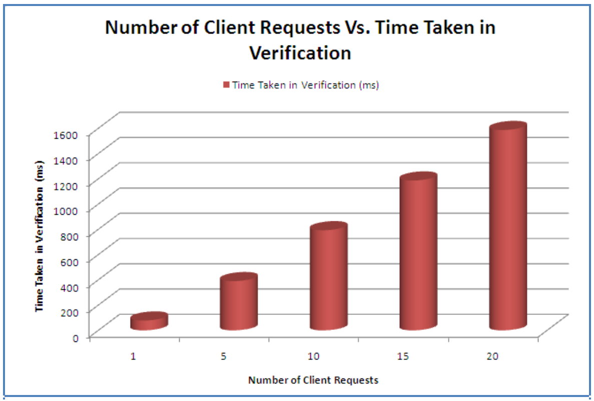


Figure 3 : Graph showing time requirements for verification process in proposed work

From the above graph it is clear that the time requirement for verification of the clouds is almost linear or is lesser. This shows that the proposed work do not impose much loads during the verification process with the increase in number of clouds. The process is similar in case of both multi cloud environment and hybrid cloud environment.

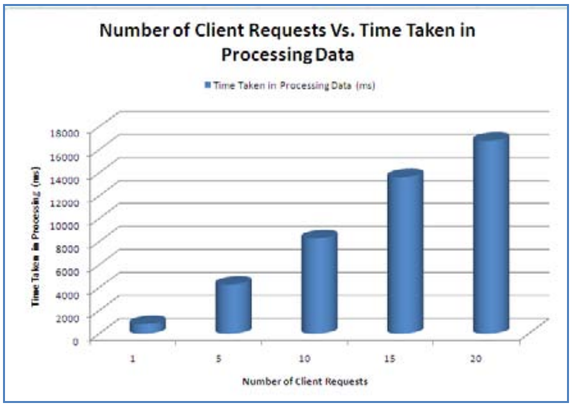


Figure 4 : Graph showing time requirements for Processing of data after verification process in proposed work

From the graph in figure 4 time taken in processing of data after verification process is completed is shown. The graph shows that as the number of clouds increase and the data transferred between them is also increased and it results in linear increase in time with the number of clouds. This is also as per the expected outcome over the cloud environment.

Table 1 show the comparison of the works of the various researchers including the proposed work and from the table it is seen that the proposed work provides better number of services in terms of cloud security. It supports multi-clouds and hybrid cloud and provides both the data and storage oriented services.

Table 1 : Comparison between the proposed work and the work of the various researchers

			Addressed Security Risks				Type Of Cloud		Type Of Service	
Ref	Year	Cloud Security	Data Integrity	Data Intrusion	Service Availability	Privacy/ Security Mechanism	Single Cloud	Multi Clouds	Cloud Storage	Cloud Database
Proposed Work	2013	√	√	√	√	Multi shares+ secret sharing algorithm		√	√	√
[5]	2011	√	√			Multi shares+ secret sharing algorithm				
[8]	2011	√	√	√	√	DepSky,(Byzantine + secret sharing + cryptography)		√	√	
[42]	2011	√ survey	√				√		√	
[3]	2010	√				RAID-like techniques+ introduced RACS		√	√	
[11]	2010	√	√			ICStore,(clientcentric distributed protocols)		√	√	
[17]	2010	√			√	SPORC, (fork)	√			
[22]	2010	√								
[25]	2010					cryptography	√		√	
[30]	2010					Depot, (FJC)				
[48]	2010	√	√			Venus	√		√	
[49]	2010	√ survey	√		√		√		√	
[51]	2010	√					√		√	
[52]	2010	√	√				√		√	
[10]	2009	√	√		√	HAIL (Proofs + cryptography)		√	√	
[12]	2009	√ survey	√					√	√	
[16]	2009	√	√			encrypted cloud VPN	√		√	
[41]	2009	√					√		√	
[43]	2009	√	√		√	TCCP	√		√	
[55]	2009	√	√			homomorphic token + erasure-coded	√		√	
[7]	2007		√			PDP schemes				
[19]	2007	√					√		√	

V. Conclusion and Future Work

Since cloud connects to thousand and thousand people over internet or intranet on pay per basis, therefore security of the cloud is a focused are for researchers and with the growth of the cloud computing and hybrid computing, requirements for security are increasing heavily. The proposed work is expected to provide a good security infrastructure over cloud.

One mechanism is to share the challenge text between the clouds before actual communication should start for authentication. The various works done in this area till date are oriented on other techniques of security between the two or more clouds in a hybrid cloud.

Cloud Computing is facilitating users around the world for the best of the services available across the world on their machines through web. It is beneficial for both the service providers (they get huge clientele) and clients (they get all available services).

For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services.

References Références Referencias

1. Safwan Mahmud Khan and Kevin W. Hamlen, “Hatman: Intra-cloud Trust Management for Hadoop”, 2012 IEEE Fifth International Conference on Cloud Computing, 978-0-7695-4755-8/© 2012 IEEE DOI 10.1109/CLOUD.2012.64
2. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds” 2012 45th Hawaii International Conference on System Sciences 978-0-7695-4525-7/12 © 2012 IEEE DOI 10.1109/HICSS.2012.153
3. Deyan Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing” 2012 International Conference on Computer Science and Electronics Engineering 978-0-7695-4647-6/12 © 2012 IEEE DOI 10.1109/ICCSEE.2012.193
4. Zhang Yandong, Zhang Y ongsheng, “Cloud Computing and Cloud Security Challenges” 2012 International Symposium on Information Technology in Medicine and Education.
5. Fan, Chih-Tien; Wang, Wei-Jen; Chang, Yue-Shan; High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on Publication Year: 2011, Page(s): 887 – 892.
6. Gul, I.; ur Rehman, A.; Islam, M.H.; Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on Publication Year: 2011, Page(s): 143 – 148.
7. Mazhelis, Oleksiy; Tyrvainen, Pasi; Software Engineering and Advanced Applications (SEAA), 2011 37th EUROMICRO Conference on Digital Object Identifier: 10.1109/SEAA.2011.29 Publication Year: 2011, Page(s): 138.
8. Research on Cloud Computing Security Problem and Strategy Wentao Liu Department of Computer and Information Engineering, Wuhan Polytechnic University, Wuhan Hubei Province 430023, China 978-1-4577-1415-3/©2012 IEEE
9. Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue “Security Issues and Solutions in Cloud Computing “, 32nd International Conference on Distributed Computing Systems Workshops, 1545-0678 © 2012 IEEE DOI 10.1109/ICDCSW.2012.20
10. Chunqing Chen, Shixing Yan, Guopeng Zhao, Bu Sung Lee, “A Systematic Framework Enabling Automatic Conflict Detection and Explanation in Cloud Service Selection for Enterprises”, 2012 IEEE Fifth International Conference on Cloud Computing, 978-0-7695-4755-8 © 2012 IEEE DOI 10.1109/CLOUD.2012.95
11. Jianyong Chen, Yang Wang, and Xiaomin Wang “On-Demand Security Architecture for Cloud Computing “, 0018-9162 © 2012 IEEE
12. Iliana Iankoulova, Maya Daneva, “Cloud Computing Security Requirements: a Systematic Review”, 978-1-4577-1938-7 ©2011 IEEE
13. Eman M.Mohamed, Hatem S. Abdelkader, Sherif El-Etriby, “Enhanced Data Security Model for Cloud Computing”, The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May, 2012.

This page is intentionally left blank