RECENT TRENDS AND ISSUES ON THE INTERCLOUD AND DEPENDABLE STORAGE

[1] R. PRAVEEN, [2] GEORGE GABRIEL RICHARD ROY
[1] STUDENT, [2] ASSISTANT PROFESSOR
[1] DEPARTMENT OF INFORMATION TECHNOLOGY,
[1] St. JOSEPH'S COLLEGE (AUTONOMOUS), TRICHY-620 002, INDIA.

Abstract : ***Cloud computing has a potential to transform a way of outsourcing and sharing business activities in a dynamic world. The current cloud computing enables clients to interact with servers and it provides infinite scalability and depends on availability towards changing of systems and services. However, cloud computing proliferation have not lived and comes in the enterprise segment. Often issues including in these computing be confidentiality and integrity, but also reliability and consistency. In this paper, we discuss about cloud computing security issues and challenges and also design the Intercloud storage which is currently are implementing, dependable services in the Intercloud. Offering a goal of building in services and systems are more dependable. Intercloud layer, client-centric distributed protocols complement are more provider-centric, large-scale ones in the Intracloud layer. Intercloud Storage precisely addresses and improves the CIRC attributes which means confidentiality, integrity, reliability and consistency of cloud storage services.***

IndexTerms - Intercloud; CIRC; Client-centric protocols.

I. INTRODUCTION

Cloud computing act as promising model to the client, infinite scalability and always-on availability[1], that makes renders in appealing of data for use and computation outsourcing for services and systems, both for consumers want to share their pictures with friends and for enterprises world to reduce their IT budgets and costs. They obvious on dependability and security concerns associated potentially under untrusted third-party. Eventhough some cases if the cloud provider is itself trusted by the client, issues may be occurs be like multi-tenancy entail vulnerabilities. More specifically, problems occurs in data confidentiality and integrity, but also reliability and consistency of the contracted service. We trust that a promising solution for improved cloud security and dependability be in the Intercloud, goes beyond adding perfection to single, the cloud of clouds in computing, isolated cloud computing. In this paper, we first discuss about cloud security issues and challenges in cloud. Secondly, design of a service in the Intercloud storage, exploits the unique features of this model: storage service that is currently under development and addresses the CIRC dimensions through a layered architecture.

II. CLOUD SECURITY ISSUES

Information Technology business environment one of the major issues is security. Customers and users using of grid computing to cloud according to their business, issues emerged due to the risk of losing customer data.

A) VIRTUAL SECURITY ISSUES

The most sensitive and important part of cloud is virtual security [2]. It runs and manages the IT infrastructures in the cloud. The other problems are non-secure apps and vulnerability.

1) Network Attacks in Virtual cloud:

Different virtualization [3] products can running increasing of attackers perimeter. The attackers may hacked the data and shut down based on attacks to disturb 1000millions of services as a disrupt.

2) Distributed Denial of Service (DDOS) Attacks:

Target at networks and servers. In the worst cases, the attackers will use botnets to perform DDOS [4] which is helpful in hacking the network.

3) Non-Secure Apps:

It is an complicated issue, because of if the customers or users may ignore securing of data it been deploying before in cloud computing [5].

4) Domain Name Server (DNS) Attacks:

It can easily attack the attackers when they call the server by name. Using the IP address is not always feasible in DNS [6].

B) PHYSICAL SECURITY ISSUES

In this security issues, data may be occurs in virtual server, it can be stored in cloud in the form of machine issues and storage [7]. While the issues can be protected by both insider and outsider attackers.

1) Loss of Physical Control:

It occurs when the customers join the cloud either by keeping their app in cloud.

a) Privacy and Data:

This rises multiple legal concerns as the customers premises is not available [8].

b) Control over Data:

It been customers confidence to control over data, its provider offers services for appropriate controls.

c) Legal and Regulatory Compliance:

In these types of issues, customers expert providers to build or focus on cloud to address the needs of certificate and trust confidentiality.

2) Human Attacks:

It occurs when unauthorised person tries to access datacentre [9, 10]. It is a kind of attacks. For example – The cloud provider losing their significant control.

3) Power Failure:

In this issues, cloud failure faced many problems because of power failure, disaster recovery.

III. CLOUD SECURITY CHALLENGES

The concept of risk management is the heart of security and privacy. These factors become a critical element affecting security in business world and organizations for customers and cloud providers. The cloud provider is facing a lot of security issues and they always try to mitigate leaks in their security system.

A) Trust Management:

It ensures the customer feels secure and safe. The idea of trust management is based on having a mutual trust between providers and customers [11].

B) Rapid Elasticity:

It manage and monitors request to guarantee implementing the private could environment. It ensures maximum flexibility for the customers [12]. It should present the allocations and ensures the limit of resources.

C) Transparency:

Cloud providers does not expose of their internal policy, customer trust in cloud provider's security claims [15]. Customers and users should have their privacy, cloud security and managed of data.

D) Virtualized Datacenter:

Customers have run on highly virtualized datacentre [11], cost has been driven up in many areas, very expensive servers. Virtualization was under savings on physical hardware, rapid return on environment can be realized.

IV. DEPENDABLE INTERCLOUD STORAGE

ICStore client consists of three layers that goals different dependability aspects:-
They are, i) confidentiality, ii) integrity and iii) reliability and consistency (RC).

i) Confidentiality

The client performs a simple symmetric key (both sender and receiver having same keys) encryption of the data and received from the client. The challenge in this layer is to be an key management. When a key is split it share with secret shared [13]) upon encryption, and key shares are been in metadata to individual clouds. Shares of data needed then reconstruct the key is to be in parameter that depends on the number of available clouds and reliability protocols.

ii) Integrity

This layer is against unauthorized data modification [6]. When a single client accesses the untrusted cloud storage, data integrity can maintained the data, while multiple clients access some data maintained by ICstore.

iii) Reliability and Consistency (RC)

The RC layer consists of fault-tolerant distributed protocols that disperse data to the Intercloud. After the data can passes through the confidentiality and integrity layers [9]. Support a variety of data dispersal protocols which are to be selected depending on the goals of the end application. In addition of increased cost of such an approach, this raises issues regarding access control on base clouds. The trends are present in recent single-domain cloud storage implementations. The final stage of these implementation is plan to add an extra coding to client-driven storage protocols.

V. CONCLUSION

Finally we addressed and surveyed some of the issues and challenges in cloud computing security and selecting the best solution for solving authentication and trust security issues. Future work will concentrate on investigating the other security issues in the Inter-Cloud federation such as security issues for implementing trust relationship between platforms and infrastructures as storage of intercloud issues solution can be maintained such as such as confidentiality, integrity, reliability and consistency. Future outcomes be in complete the implementation of ICStore prototype and evaluate of its cost and benefits.

REFERENCES

[1] H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: A case for cloud storage diversity," in ACM SoCC, 2010. To appear.

[2]H. Attiya, A. Bar-Noy, and D. Dolev, "Sharing memory robustly in message-passing systems," J. ACM, vol. 42, no. 1, pp. 124–142, 1995.

[3]Kelly Jackson Higgins, "Cloud-Based CryptoCracking tool to be unleashed at black hat DC",http://www.darkreading.com/authentication/167901072/security/encryption/229000423/cloud-based-crypto-cracking-toolto-be-unleashed-at-black-hat-dc.html, January 10, 2011.

[4]W. Stallings, Network Security essentials Applications and Standers, New Jersey, Prentice Hall, 2011.

[5]JohnKinsella, "5 more key cloud security issues", http://www.csoonline.com/article/717307/5-more-key-cloudsecurity-issues?page=3, Sep 26, 2012.

[6]Diana Kelley, "Cloud computing security: Routing and DNS security threats", http://searchcloudsecurity.techtarget.com/tip/Cloudcomputing-security-Routing-and-DNS-security-threat, June 2009.

[7]Cloud security challenges (Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on Digital Object Identifier: 10.1109/TSSA.2012.6366028), Page (s): 88 – 91) 2012.

[8]Springer Link, "Privacy by Design: essential for organizational accountability and strong business practices", http://www.globalprivacy.it/Allegati_Web/57C2B8AA758546 A0B76D5668F5CF5E16.pdf, 2010.

[9]R. Gellman, "Privacy in the louds: risks to privacy and confidentiality from Cloud Computing," World Privacy Forum, Feb. 2009.

[10]J. Szefer, P. Jamkhedkar, Y. Chen, R. Lee, "Physical attack protection with human-secure virtualization in data centers", in Proc. The 2012 IEEE/IFIP42nd International Conference on Dependable System and Networks Workshops (DSN-W'12), Boston, pp. 1-6, June 25-28, 2012.

[11]Microsoft White Paper, "Datacenter Virtualization", http://social.technet.microsoft.com/Search/enUS?query=virtualization%20datacenters%20with%20author& refinement=90&beta=0&ac=5, pp. 1-27, June 2008.

[12]Microsoft TechNet, Wiki, "Cloud Security Challenges",http://social.technet.microsoft.com/wiki/contents/articles/6651 .cloud-security-challenges.aspx, Jun 6, 2012.
[13] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[14] R. Bifulco, R. Canonico, G. Ventre and V. Manetti, "Transparent migration of virtual infrastructures in large datacenters for Cloud computing", in Proc. The 2011 IEEE Symposium on Computers and Communications (ISCC'11), Kerkyra, pp. 179 - 184, June 28 -July 1, 2011.
[15] J. A. Garay, R. Gennaro, C. S. Jutla, and T. Rabin, "Secure distributed storage and retrieval," Theor. Comput. Sci., vol. 243, no. 1-2, pp. 363–389, 2000.