ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Designing an Application for Recovery of Data in Cloud Environment: A Problem Definition

Anand Padwalkar[1]
M.Tech, CSE ,
TGPCET, Mohgaon,
Nagpur - India

Sulabha Patil[2]
Prof., TGPCET,
Mohgaon, Wardha Road,
Nagpur - India

Neha Mogre[3]
Prof., TGPCET,
Mohgaon,Wardha Road,
Nagpur - India

Abstract: ***Cloud computing recovery issues requirements have been addressed in publications earlier, but it is still difficult to estimate what kinds of requirements have been researched most, and which are still under researched. This paper carries out a systematic literature review by identifying cloud computing security requirements from publications between last recent years. It will categorize these requirements in a framework and assess their frequency of research. The paper will then identify changes in the assessment of requirements and proposed solutions compared to publications prior research work. Backing up our databases to the public cloud is an important strategic focus for us going forward in order to save money, scale our backup and DR operations, and to ensure our applications are always available to customers and business users worldwide. Over the past few years, many organizations have started to deploy public cloud for backup and Disaster Recovery (DR). Data recovery approaches with respect to digital forensics can be introduced for the sake of data management after a system encounters with an attack or any disaster like crash of vital data. These approaches often used by organizations to experience the reactive majors after a crash of data. Cloud-based business flexibility can provide an attractive alternative to traditional disaster recovery, offering rapid recovery time associated with a dedicated infrastructure and the reduced costs that are consistent with a data recovery model.***

This paper discusses one of the traditional approach to disaster recovery and describes how organizations can use cloud computing to help plan for both the routine interruptions to service— server hardware failures ,cut power lines, and security breaches—as well as more-infrequent disasters. The paper provides key considerations for the transition of replicas once a peer in the system encounters an attack in the private cloud-based business resilience. That is, a machine, once experiences calamity like instance failure of data and so on, Disaster Recovery (DR) can be carried out by an application discussed in this paper to recover the data by extracting a last Restore Point (RP). These RPs can be maintained in the stack provided with the separate system space and can be used as and when required for resilience of system in private based cloud environment.

Keywords: Cloud Computing, Security Requirements, SaaS, Software as a Service, Literature Review, Change, Security factors, Disaster Recovery (DR).

I. INTRODUCTION

Cloud Computing (CC) is a new term given to a technological evolution of distributed computing and grid computing. CC has been evolving over a period of time and many companies are finding it interesting to use. Without the development of ARPANET (Advance Research Projects Agency Network), CC would never have come into existence. The advent of

ARPANET, which helped to connect (for sharing, transferring, etc.) a group of computers, lead to the invention of Internet (where bridging the gap between systems became easy) **[1]**.

Disaster recovery has traditionally been an insurance policy that organizations hope not to use. In contrast, private cloud-based business resilience can actually increase IT's ability to provide service continuity for key business applications. The recovery tools that can be used to recover the data after a crash can be carried out by means of "Digital Forensics". These tools act as recovery major for extracting all the recent replicas from stack maintained from external repository. This paper actually deals with the development of such application when the data is lost due to some unavoidable reasons. The data damaged on particular client in private cloud environment can be managed through this application with the help of their image replica management over certain period of timestamp or once it is shutdown.

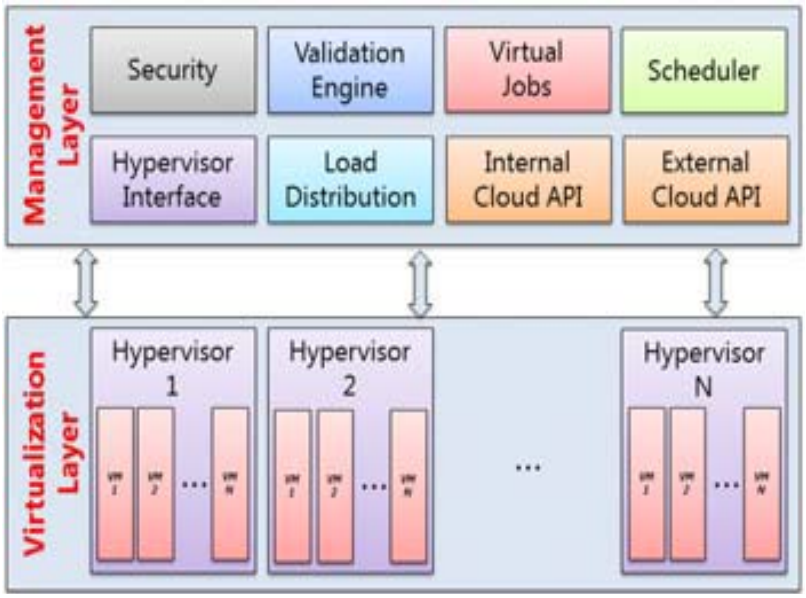


Fig1: Basic Cloud Computing Architecture [2]

II. Background and Existing Tools for Implementing DR (Disaster Recovery)

In an earlier work, Iankoulova and Daneva [10] already approached a systematic review on cloud security requirements. With this paper, the aim to be followed up on their research, taking into account the change on this topic due to aggrandizement in recent years and thus analyze to what extent the focus on requirements has shifted and derived into new issues and challenges in that field. Based on the literature available for constructing DR tools, the environment like VMWare provides the virtualization to manage the data once it encounters a DNA (Distributed Network Attack).These DNAs can be network modification of data, Corruption of Network Files etc.

Existing Tools for recovery of data when a system encounter an attack in cloud environment [11]:

1. VMWares: For virtualization and use of Hypervisor for data control
2. EnCase: Acquisition and analysis (while maintaining state), Data recovery.
3. LinkAlyzer: analyzing link files.
4. PmExplorer: GSM Key decoder.

Based on the existing tools' functionalities and procedures, this application will analyze the private cloud environment for data recovery and supervise all the controls at hypervisor level. The hypervisor will be maintaining the state of all the participants in the private cloud system, that is, it will be maintaining all the transactions and transition of data carried out through all the peers in the system. The application discussed in this paper will be based on emulator VMWares (a software which provide cloud and virtualization services.)[3].

Digambar Powar,G. Geethakumari, BITS-Pilani, Jawaharnagar, Shameerpet, Hyderabad[7], emphasized on finding and analyzing digital evidence in virtualized environment for cloud computing using traditional digital forensic analysis techniques. They have also focused on basic services of cloud through which the data recovery considerations can be obtained.

More research is required in the cyber domain, especially in cloud computing, to identify and categorize the unique aspects of where and how digital evidence can be found. End points such as mobile devices add complexity to this domain. Trace evidence can be found on servers, switches, routers, cell phones, etc. Digital evidence can be found at the expansive scenes of the crime which includes numerous computers as well as peripheral devices...To aid in this quest, digital forensics standards and frameworks for digital forensics technologies are required now more than ever in our networked environment [11].

FAULT TOLERANCE TECHNIQUES	POLICIES	PROGRAMMING	ENVIRONMENT	FAULT DETECTED	APPLICATION ON TYPE
Replication	Reactive/ Proactive	Java	Virtual Machine	Process/node failures	Load balancing Fault Tolerance
Check pointing	Reactive	SQL ,Java	Virtual Machine	Application Failure	Fault Tolerance
Replication	Reactive/ Proactive	Amazon	Cloud Environment	Application/node failures	Load balancing , fault tolerance
*Replica Management	Reactive	Java	Private cloud Environment	Node Failure	Fault Tolerance

*Application discussed in this paper

Table: Existing System to implement fault tolerance and DR in cloud Environment [10]

III. Proposed Cloud Virtualized System Architecture and Implementation

A few techniques currently exist for autonomic fault tolerance in cloud environment. Virtualization is achieved through hypervisor to secure the setup the connectivity between virtual clients and a server. The paper also stipulates the requirement of all the clients connected to the server in private cloud setup like static IP address and monitory configuration of the system.

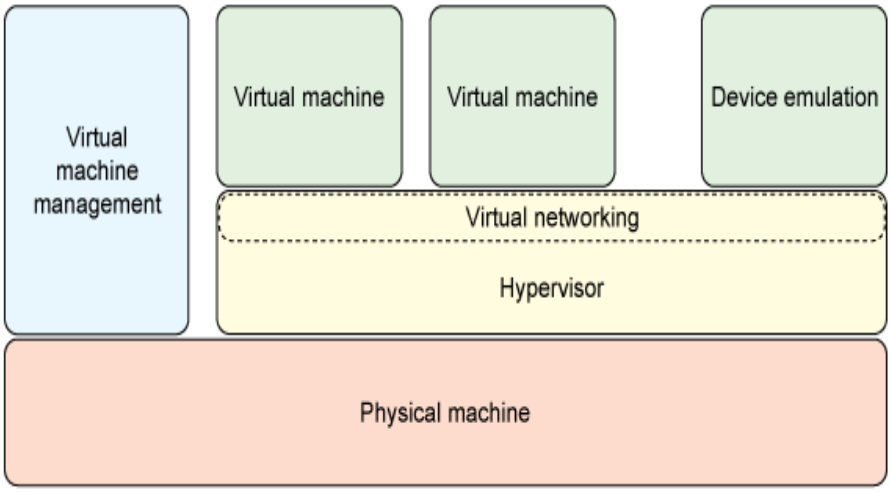


Figure: Cloud Virtualized System Architecture

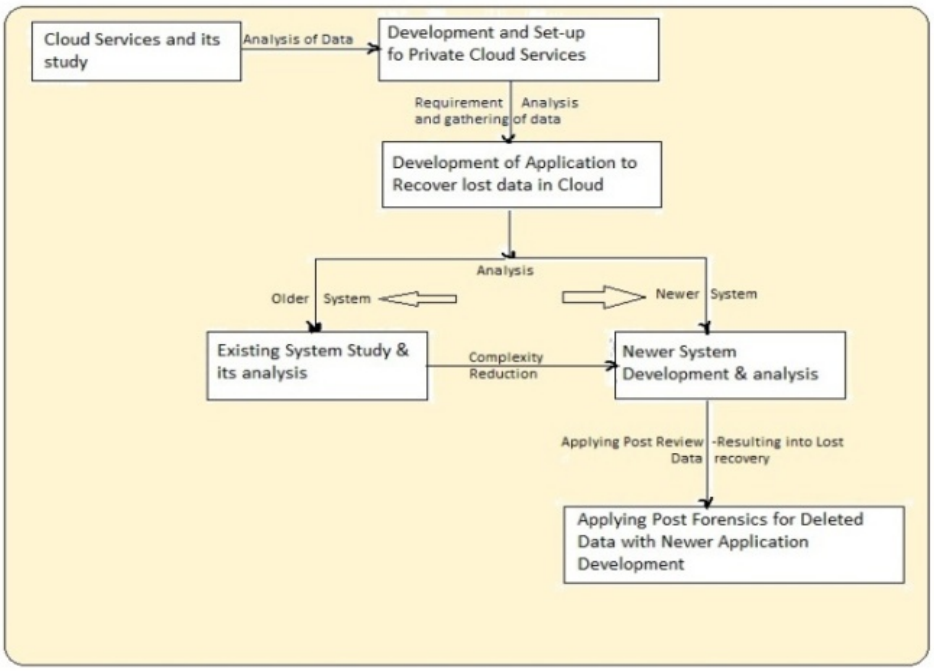
These replicas can be maintained through the stack collection and if any damaging circumstance happens, in that moment of time latest replica can be overruled on that particular client.

A machine (Client) is said to be encountered with an attack in the following conditions:

1. If a machine (client) in a cloud environment stops responding to server (while pinging).

2. If a machine stops responding to neighboring machine (static pinging scheme will be implemented for private cloud environment to practice.
3. If a machine encounters an attack with the reasons like an abnormal shutdown, prologue of malicious programs (malwares, viruses, Trojans etc) and an inappropriate booting of client machine.

The proposed work is planned to be carried out in the following manner



IV. CONCLUSION

Disaster tolerance is implemented dealing with various software faults for server applications in a cloud virtualized environment. When one of the servers goes down unexpectedly, connection will automatically be redirected to the other server Data replication technique is implemented on virtual machine environment [10]. The experimental results are obtained, that validate the system fault tolerance.

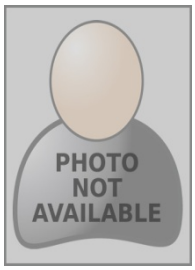
References

1. Kaleem Ullah and M. N. A. Khan," Security and Privacy Issues in Cloud Computing Environment: A Survey Paper", International Journal of Grid and Distributed Computing Vol.7, No.2 (2014), pp.89-98 http://dx.doi.org/10.14257/ ijgdc.2014.7.2.09
2. Deoyani Shirkhedkar, Sulabha Patil ," DESIGN OF DIGITAL FORENSIC TECHNIQUE FOR CLOUD COMPUTING"2014 , IJARCSMS All Rights Reserved 192| P a g e ISSN: 2321 -7782 (Online) Volume 2 , Issue 6 , June 2014.
3. Alecsandru Pătraşcu, Victor-Valeriu Patriciu, "Logging System for Cloud Computing Forensic Environments", CEAI, Vol.16, No.1 pp. 80-88, 2014.
4. Parag Shende And Prof.Sulabha Patil, "ENHANCING PRIVACY IN INTERCLOUD INTERACTION", Proceedings of 7th IRF International Conference, 27th April-2014, Pune, India, ISBN: 978-93-84209-09-4.
5. M.Usha, "A Study on Forensic Challenges in Cloud Computing Environments", Vol 2 | Issue 3 | Spring Edition | DOI : February 2014 | Pp 291-295 | ISSN 2279 – 0381
6. NM Karie, HS Venter – 2013, "An Ontological Framework for a Cloud Forensic Environment", Proceedings of the European Information Security Multi-Conference (EISMC 2013), 1Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield 0028, Pretoria, South Africa.
7. Digambar Powar, BITS-Pilani, Jawaharnagar, Shameerpet, Hyderabad, G. Geethakumari BITS-Pilani, Jawaharnagar, Shameerpet, Hyderabad," Digital Evidence Detection In Virtual Environment For Cloud Computing", Pages 102-106 ACM New York, NY, USA ©2012
8. Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd," A Survey About Impacts of Cloud Computing on Digital Forensics", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94 The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)
9. Farzad Sabahi, Member, IEEE," Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.
10. Fault Tolerance- Challenges, Techniques and Implementation in Cloud Computing, by Anju Bala1, Inderveer Chana, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012,ISSN (Online): 1694-0814 www.IJCSI.org
11. Lohr, Steve (2009-08-31). "VMware market share more than 80%". The New York Times. Retrieved 2010-05-27

AUTHOR(S) PROFILE

Anand R. Padwalkar is pursuing, Master of technology in Computer Science and Engineering from TGPCET of Rashtrasant Tukadoji Maharaj Nagpur University. Till now, he has authored and over 10 (Ten) publications in International, National and various conference proceedings. He holds Life Member of ISTE, New Delhi (LM-66529). His publications include "Network Security Concerns", "Secured Multiparty Trusted computation protocol and its various approach", "TTPs' (Trusted Third Party) Role in data mining, Cloud Security Concerns" and so on.

Prof. Sulabha Patil is Head, Mohan Gaikwad Invention & Research Centre and an Assistant Professor in department of Computer Science and engineering. She is currently holding the charge of Deputy Editor of Journal of Emerging trends in Science & Technology is an online e-journal of Gaikwad-Patil Group of Institutions. She is having teaching experience over 20 years in the computer Science field. She is also puring her PhD in the same domain. She has guided number of M.Tech students till now in the Cloud Computing Area, Network Security Concerns and Wireless Communication and Computing Domain.



Prof. Neha Mogre is an Assistant Professor, in Department of Computer Science and Engineering, in Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur. She has completed M.Tech in CSE and pursuing her PhD in the same stream. She is having 5 years of teaching experience in the same field. She has guided number of M.Tech students till now in the Cloud domain and Network Security Concerns.