Designing an Application for Recovery of Data in Cloud Environment: A Literature Review

Anand Padwalkar
M.Tech, CSE,
TGPCET, Nagpur
anandpadwalkar@gmail.com

Prof. Sulabha Patil
Prof., Tulsiramji Gaikwad-Patil College of Engg. & Tech., Nagpur,
sulabhavpatil@gmail.com

Prof. Neha Mogre
Prof., Tulsiramji Gaikwad-Patil College of Engg. & Tech., Nagpur,
neha.cse@tgpcet.com

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). Most enterprises using public cloud find significant cost savings on storage, improved IT productivity, and agility to support new database backup and DR requirements. The paper will be based on the research work carried over the different aspects of DR and surveys based on different modules of designing of an application to recover the data in cloud environment.

Keyword: 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]**. This Internet helped to accelerate number of activities such as human interaction (social media, instant messaging, etc.), business needs of an organization (online shopping, financial services, etc.). Further advancement in this area of Internet resulted in development of Applications Service Provision (ASP), grid and utility computing and cloud computing. CC introduced a new paradigm which changed the traditional interconnection of systems to a pool of shared resources that can be accessed through internet.

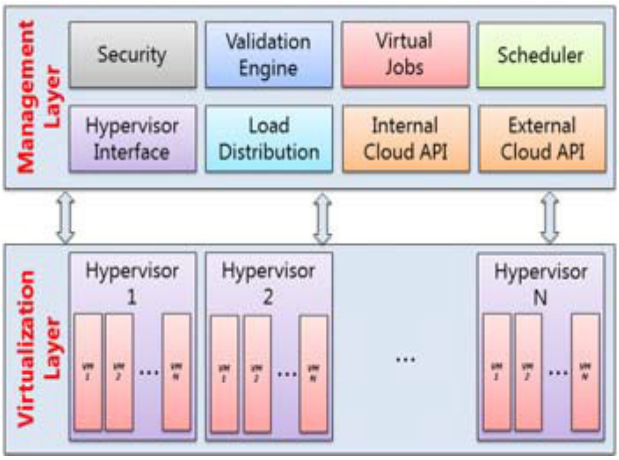


Fig1: Basic Cloud Computing Architecture

NIST (National Institute of Standards and Technology) defines cloud computing as follows: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction", as shown in fig 1 . This definition clearly states that CC helps in minimizing an organization's expenditure towards

managing resources and also reduces the burden of maintaining software or hardware by its user**[2]**. When burden of management, maintaining a software/hardware is reduced, the companies expenditure and time spent towards infrastructure management is reduced and time saved can be utilized in doing some creative work.

II. OBSERVATIONS OF RELATED WORK

In an earlier work, Iankoulova and Daneva[12] 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.

NM Karie, HS Venter[6] have focused on ontological framework meant to provide a structure and depiction of the different cloud environments and components an investigator should be acquainted with, in the case of a cloud investigation process. In addition, the relationships and interactions between the different environments by capturing their content and boundaries are also shown in this paper regarding the security area of cloud computing. Furthermore, the purpose of this paper is meant to provide a common ontological framework for sharing coherent cloud computing concepts and also promote the understanding of the cloud environments and cloud components regarding to Cloud Forensics.

Rainer Poisel ,Erich Malzer and Simon Tjoa[20] have described the challenges and opportunities for scientific developments in the field of cloud forensics. In this paper, the detailed description of digital forensics investigations at the hypervisor level of virtualized environments in greater detail is taken into considerations for Recovery of Data in cloud Environment.

Josiah Dykstra and Alan T. Sherman, Cyber Defense Lab, Department of CSEE [13], have emphasized on the model to show the layers of trust required in the cloud. Secondly, they have presented the overarching context for a cloud forensic exam and analyze choices available to an examiner. Also for the first time they have proposed an evaluation of popular forensic acquisition tools including Guidance EnCase and AccesData Forensic Toolkit, and shown that they can successfully return volatile and non-volatile data from the cloud

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.

Deoyani Shirkhedkar and Prof. Sulabha Patil [2] have proposed digital forensic technique for cloud environment which will detect two attacks DDOSs and unauthorized file sharing. This paper also emphasizes on forensic investigation techniques of data by taking into consideration of digital object.

Farzad Sabahi, *Member, IEEE,* [9] have focused on new security architecture in a hypervisor-based virtualization technology in order to secure the cloud environment virtualization technology is built on virtualization technology which is an old technology and has had security issues that must be addressed before cloud technology is affected by them. The paper also emphasizes on relation between reliability and security in virtualization, virtual machines security threats and attacks in virtualization

Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez [10] have analyzed the security issues by identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing. In this paper the Systematic review of security issues for cloud computing are discussed like Application Security, Multi-Tenancy, Third party Relationships and solutions to mitigate the treats and vulnerabilities in Cloud environment.

Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd[10], have identified a cross-disciplinary approach between cloud forensics, digital forensics and cloud Computing. This paper also shown the role trusted third parties and the cloud service providers'perspectives and has explained whether they can gain the authority to get access to the evidence. And finally, for service providers' point of view this paper has summarized whether they able to guarantee the safety of the data.

Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud, Solahuddin bin Shamsuddin[15] have discussed about the concept of cloud computing, as well as forensic investigation practices; knowing both, brings the cloud forensic investigation issues to light. This article illuminated some of the conflicts of digital forensic investigation and cloud environment; and then continued with discussing some of the possible solution.

Ashalatha R[21] has provided a comprehensive review on the essentiality of Security- as- Service in cloud computing scenario. The paper also presents the significance of data security and the various existing security techniques for the cloud. This paper also focuses on security issues encountered in cloud computing.

Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem[16] explored the importance of the cloud computing and risks associated with the cloud computing procedure and process. This paper also illustrated the data privacy problem in cloud computing environment. Different data protection models and techniques have been defined that show their contribution in cloud computing. This paper provided a base for future research work in the field of data security of cloud computing system.

Alecsandru Pătraşcu, Victor-Valeriu Patriciu[3] presented a novel solution that provides to the digital forensic investigators a reliable and secures method in which they can monitor user activity over a Cloud infrastructure. The paper also has focused on increasing reliability, safety, security and availability of Cloud Computing systems. The characteristics of such systems present problems when tackling with secure resource management due to its heterogeneity and

geographical distribution an also presented the design of a hierarchical architectural model that allows investigators to seamlessly analyze workloads and virtual machines, while preserving scalability of large scale distributed systems.

Parag Shende And Prof.Sulabha Patil[4] have described describes an emerging approach, called user centric identity management that focuses on usability and cost effectiveness from the user's point of view. This paper also analyzed the challenges posed by cloud computing and the standardization work being done by various standards development organizations (SDOs) to mitigate privacy risks in the cloud, including the role of privacy enhancing technologies (PETs).

M.Usha [5] focused on the technical aspects of digital forensics in distributed Cloud environments. It contributes by assessing whether it is possible for the customer of Cloud computing services to perform a traditional digital investigation. This paper discussed the techniques to collect the crime evidences that have been conducted through computers. This paper also involves the definition of cloud computing along with forensic & its vivid types involved in computer forensic.

Chiang Ku Fan and Tien-Chun Chen, Shih Chien University [17] have focused on "Cross-Cloud Compatibility. The findings also revealed that people who work in the field of information or Cloud Computing are somehow ignorant of where the risks in Cloud Computing lie due to its novelty and complication. The major contribution of this paper lies in the identification and verification of Cloud Computing services' risk factors.

Mohsen M. Doroodchi, Amjad Ali [22] examined the forensics as a scientific discipline, in addition to the traditional view, and analyzes the past and future trends of its models. Furthermore, key characteristics of a framework for next generation uniform models that are adaptable to computer science discipline are identified. The proposed model in this paper incorporated certain features of the past models to provide a new framework. In particular, the ontology of current computer technology in addition to abstraction layers of forensic science used to provide the structure of this model.

George SIBIYA, Hein S. VENTER and Thomas FOGWILL [18], have examined a framework aimed at addressing digital forensics challenges in a cloud environment. The framework addresses the issue of data acquisition in the cloud that may be beyond the jurisdiction of investigators. It makes use of accessible information to build up a case before the costly data acquisition from foreign countries could be carried out.

Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir[8] , Nor Fazlida binti Mohd Sani and Solahuddin bin Shamsuddin, Farhood Norouzizadeh discussed in their review paper , the cross-disciplinary approach between digital forensics and cloud computing. The discussion is basically on the security problems when digital forensics analysis is embedded into cloud computing environments. The paper also discussed the progression of connectivity, the flat corporate network and the social engineering path. This may be one of the future works in the cloud computing field.

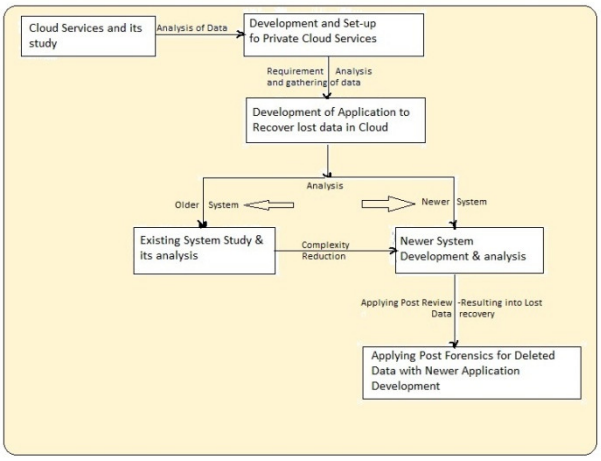
F. A. Alvi, B.S Choudary, N. Jaferry and E.Pathan[23], in their review paper about cloud security and its challenges, have discussed and addressed the issues that can arise during the deployment of cloud services. After identify these problems some steps are explained to mitigate these challenges and solutions to solve the problems.

Josiah Dykstra and Alan T. Sherman described the design [23], implementation, and evaluation of FROST: three new forensic tools for the OpenStack cloud platform. FROST provides the first forensic capabilities integrated with OpenStack and to our knowledge the first to be built into any infrastructure-as-a-Service (IaaS) cloud platform. FROST offers concrete user-accessible forensic capabilities to cloud consumers. While many organizations are still hesitant to adopt cloud solutions because of security concerns.

III. PROPOSED METHODOLOGY

The proposed scheme for security model in cloud computing for designing an application using soft computing technique comes across with the usage of reputation management system which is a proficient reputation collection scheme from multiple cloud nodes to ensure the data security. For enhancing the security, trust and reputation verification technique is used which is more efficient. The hypervisor security discussed in previous research includes the cloud node, timestamp, public keys of the cloud involved, trust evaluation etc. Advanced cryptography algorithm like RSA and AES along with efficient soft computing technique will be utilized for developing an application to maintain the disaster recovery (DR). The proposed method for security model in cloud computing will be implemented in the JAVA platform.

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



IV. CONCLUSION AND FUTURE WORK

Cloud Computing is in a period of strong growth, but this technology is still has some issues of security and somewhat it is immature. This paper highlights many of the forensic challenges in the cloud computing environment for the digital forensics practitioner, the cloud Provider s, law enforcement, and others. We provide a definition of cloud computing forensics to scope this area. We discuss cloud forensics

stakeholders and their roles. We examined recent research papers and involved the international community. Our categories of challenges include architecture, data collection, analysis, anti-forensics, incident first responders, role management, legal issues, standards, and training.

Cloud computing is the on demand utilization of shared computing resources available from the Internet. When these services are used properly, they can reduce cost and management responsibilities in addition to increasing efficiency, agility and performance of an enterprise. On the contrary, there are several challenges to be faced by cloud computing such as data security and privacy issues. In this paper, we have discussed the issues related to data location, storage, security, availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. For this purpose, we have surveyed some of the trust management models. Since trust is an abstract and subjective term; hence, it is difficult to measure and manage the trust. In this paper, we have conducted a review of literature on the trust management system. Majority of the proposed systems put special emphasis on the CIA (Confidentiality, Integrity and Applicability) mode.

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

V. 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] Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, "A Survey on Cloud Computing and Digital Forensics", Journal of Next Generation Information Technology(JNIT) Volume4, Number6, August 2013.

[11] Josiah Dykstra and Alan T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform" , 1742-2876/$ – see front matter ª 2013 Josiah Dykstra and Alan T. Sherman. Published by Elsevier Ltd. All rights reserved.http://dx.doi.org/10.1016/j.diin.2013.06.010 journal homepage: www.elsevier.com/locate/diin

[12] Iankoulova, I., Daneva, M. Cloud computing security requirements: A systematic review. In: Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on. 2012, p. 1-7. doi:10.1109/RCIS. 2012.6240421

[13] Josiah Dykstra and Alan T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques", Cyber Defense Lab, Department of CSEE University of Maryland, Baltimore County (UMBC) 1000 Hilltop Circle, Baltimore, MD 21250 April 18, 2012.

[14] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez," An analysis of security issues for cloud computing" , Hashizume et al. Journal of Internet Services and Applications 2013, http://www.jisajournal.com/content/4/1/5

[15] Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud, Solahuddin bin Shamsuddin, "Cloud Computing and Conflicts with Digital Forensic Investigation", International Journal of Digital Content Technology and its Applications(JDCTA) Volume7,Number9,May 2013 doi:10.4156/jdcta.vol7.issue9.65

[16] Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem, " A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing", *IOSR Journal of Computer Engineering (IOSRJCE) ISSN : 2278-0661 Volume 1, Issue 3 (May-June 2012), PP 28-36 www.iosrjournals.org*

[17] Chiang Ku Fan and Tien-Chun Chen, Shih Chien University, " The Risk Management Strategy of Applying Cloud Computing" , *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 9, 2012.*

[18] George SIBIYA, Hein S. VENTER and Thomas FOGWILL, "Digital Forensic Framework for a Cloud Environment", *IST-Africa 2012 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2012 ISBN: 978-1-905824-34-2*

[19] Santosh Bulusu Kalyan Sudia School of Computing Blekinge Institute of Technology SE-371 79 Karlskrona, "A Study on Cloud Computing Security Challenges

[20] Rainer Poisel 1, Erich Malzer , and Simon Tjoa ," Evidence and Cloud Computing:The Virtual Machine Introspection Approach" St. Poelten university of Applied Sciences St. Poelten, Austria frainer.poisel, simon.tjoag @fhstp.ac.at2 Open Networks Vienna, Austria em@ong.a

[21] Ashalatha R, "SURVEY ON SECURITY AS A CHALLENGE IN CLOUD COMPUTING", International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends in Technology (NCET-Tech)

[22] Mohsen M. Doroodchi, Amjad Ali, " Framework for Next Generation Digital Forensics Models", Center for Security Studies, University of Maryland University College, Adelphi, Maryland, USA

[23] F. A. Alvi, B.S Choudary, N. Jaferry and E.Pathan, "A review on cloud computing security issues & challanges", Corresponding Author: fizza_alvi85@yahoo.com