International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 12, December 2016
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

SECURITY TECHNIQUES FOR PROTECTING DATA IN CLOUD COMPUTING

A.Zakiuddin Ahmed[1], S.Ganesh[2] P.Rizwan Ahmed[3]

[1]Assistant Professor of Computer Science, Mazharul Uloom College, Ambur (India)
[2]Research Scholar, Mazharul Uloom College, Ambur (India)
Assistant Professor of Computer Applications, Mazharul Uloom College, Ambur(India)

ABSTRACT

From the past few years, there has been a rapid progress in Cloud Computing. With the increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users using centralized resources. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. The main aim of this research is to understand the security threats and identify the appropriate security techniques used to mitigate them in Cloud Computing. The main objectives of this research are:

- *To understand the security issues and the techniques used in the current world of Cloud Computing.*
- *To identify the security challenges, those are expected in the future of Cloud Computing.*
- *To suggest counter measures for the future challenges to be faced in Cloud Computing.*

Keywords: Challenges, Cloud Computing, Security, Techniques.

I INTRODUCTION

From the past few years, there has been a rapid progress in Cloud Computing. Cloud Computing delivers a wide range of resources like computational power, computational platforms, storage and applications to users via internet. The major Cloud providers in the current market segment are Amazon, Google, IBM, Microsoft, Salesforce, etc... With an increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. Below, we have described the two main states that hold your data is out in the Cloud: when the data is in motion (transit) and when the data is at rest, where the data is much expected to be more secure. The below illustrated are the two main scenarios which we have focused to understand the security of the data in the Cloud.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

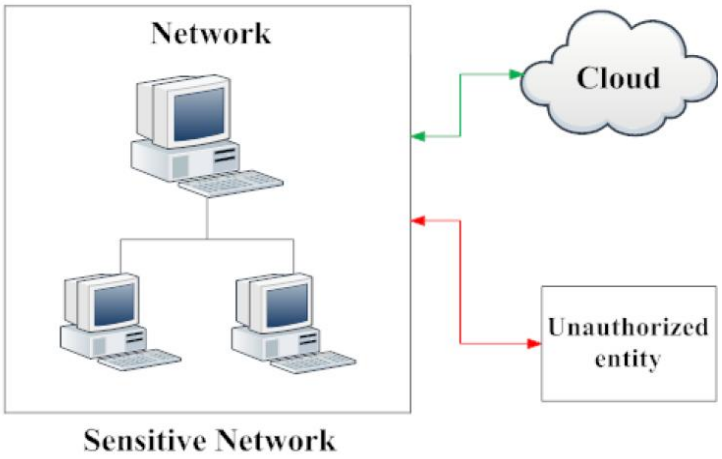

Figure 1.1 Unauthorized access of data between the network and Cloud

The above figure 1.1 describes a scenario where a local network is connected to a Cloud network, in which some part of the network data is broken out from the local network and placed in the Cloud, but the critical data resides in the local network itself. In this case, the Cloud provider does not have any privilege of accessing the data physically which is in the local network. But in some cases, the Cloud needs to access some information which is in the local network, during that access; there exists a possibility of unauthorized access of the local network resources. It describes the typical problem in network security where the information can face active attacks and passive attacks. The active attacks include masquerading, replay attack, modification of messages and denial of service. Passive attacks include traffic analysis. These attacks are likely to happen when the stream of information leaves the client network to the Cloud network.

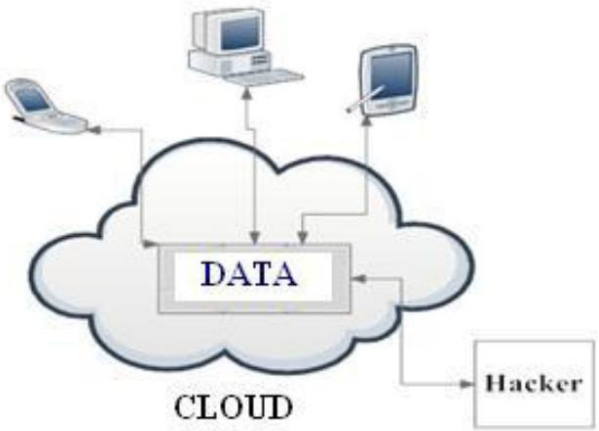

Figure 1.2 Unauthorized access of data within the Cloud

ISSN (O) 2454-9665
ISSN (P) 2454-0663

The above figure 1.2 describes the scenario where the total data of the local network resides within the Cloud, where the local network and the authorized users can access their data physically in the Cloud. At that instant of time, there exists a possibility for unauthorized users to enter and access the data in the Cloud. In this situation, the virtual machines are allotted to users of the Cloud. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways.

Regarding this area of study, most of the research papers followed a normal traditional literature survey method. Few papers gave an innovative idea and proposed a security model. However, there are very few works, which considered the opinions of various security experts in Cloud Computing. This study proposes that, reader gets the true reflection of the security practices followed by various Cloud Computing companies in the current era. There are very few papers which focus on the security techniques for specified applications. Our work provides more knowledge in this dimension and also predicts the future threats likely to be faced by Cloud Computing and solutions to these threats.

II IMPORTANT SECURITY ISSUES IN THE CLOUD

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below:

Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location .

Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP‟s) in order for their systems to have redundancy.

Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren‟t encrypting their communications.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

III RESEARCH METHODOLOGY

In this research work, we reviewed the previous work in order to acknowledge the current knowledge to answer the research questions 1 and 2. Most of the previous research works were done with traditional literature review which has low scientific value due to non- rigorous and unfair approach. Where the systematic literature review has is of highly defined characteristics with more clear scientific perspective. So we have undertaken the systematic literature review (SLR) as a primary research method, survey and interviews are considered as secondary research method. The outlook of the research methods which are used to answer the research questions is shown in figure 3.1

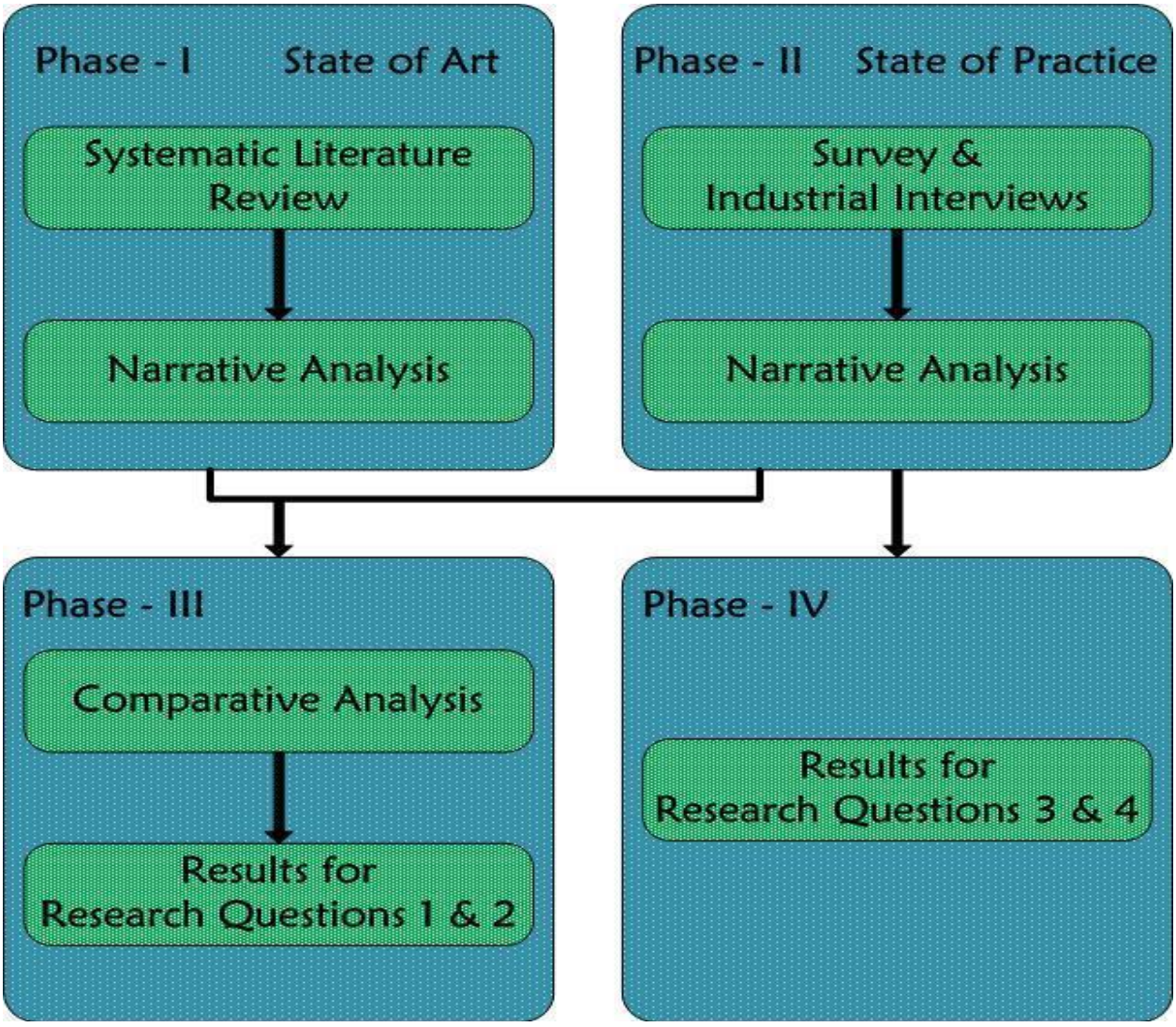

Figure 3.1 Research Design

ISSN (O) 2454-9665
ISSN (P) 2454-0663

3.1 Data Analysis Methods

Data analysis or Data synthesis is a means of collecting and summarizing the results of the studies. Data analysis methods are used to structure the data properly based on the findings. In our thesis, initially we have focused on Narrative Analysis for analyzing the results which are obtained from doing Systematic Literature Review and thereafter we have used the Comparative Analysis method for comparing the results of the SLR with the results obtained from the Survey.

3.2 Narrative Analysis

Narrative analysis is a method of non-quantitative synthesis which represents the extracted information about studies should be tabulated in a manner consistent with the review questions. Tables should be structured to highlight similarities and differences between study outcomes. It is important to identify whether results from studies are consistent with one another (i.e. homogeneous) or inconsistent (e.g. heterogeneous). Results may be tabulated to display the impact of potential sources of heterogeneity [34]. The Frame work for Narrative analysis is:

- Developing a theory
- Developing a preliminary synthesis
- Exploring relationships in the data
- Assessing the robustness of the synthesis.

3.3 Comparative Analysis

Identifying the similarities and differences in the literature with real world context can be yielded through Comparative Analysis. Qualitative Comparative Analysis (QCA) was developed by Charles Ragin . QCA was used to find the relation and dissimilarities between the contexts of study. QCA focuses on recognizing "similarities, differences, and associations between entities".

We have observed QCA fits liable to our study as we are focusing on identifying the challenges and mitigation strategies related to security in Cloud Computing both from literature and surveys.

IV CONCLUSION

The identification of security challenges and mitigation techniques in Cloud Computing is challenged by considering the large number of services. Most of the responses from survey, noted that Cloud Computing will place dominant and expandable information transactions. Because it offers many flexible services, provides easy, individualized and instant access control to the services and information where they are for the users. In the process of identification from the research methods SLR and Survey, we have identified satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

REFERENCES

1. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', *High Capacity Optical Networks and Enabling technologies (HONET)* , 19-21 Dec, pp. 190-195.

2. Ahuja R. (June 2011) 'SLA Based Scheduler for Cloud storage and Computational Services', International Conference on Computatonal Science and Applications (ICCSA), 258-262.

3. Albeshri A, Caelli W. (Sept 2010) 'Mutual Protection in a Cloud Computing Environment', 12th IEEE International Conference on High performance Computing and Communications (HPCC), 641-646.

4. Almulla S, Chon Yeob Yeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7.

5. B. lagesse. (Mar.2011) 'Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, 106-110.

6. Brenner Michel, Wiebelitz Jan. (may 31, 2011) 'Secret program execution in the Cloud applying homomorphic encryption', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference 2011, 114-119.

7. C. C Ragin. (1997) 'Turning the tables: How case - oriented research challenges variable oriented research', *Comparative social research*, vol. 16, pp. 27-42.

8. C. C Ragin. (2000) *Fuzzy set science*, Chicago: The university of Chicago.

9. Chang Lung Tsai, Uei –Chin Lin. (Aug 2010) 'Information Security issue of enterprises adopting the application of Cloud Computing', 6th International Conference on Networked Computing and Advanced Information Management (NCM), 645-649.

10. Chenguang Wang, Huaizhi Yan. (Dec 2010) 'Study of Cloud Computing security based on Private Face Recognition', International Conf. on Computational Intelligence and Software Engineering , 1-5.

11. Cong Wang, Kui ren. (2010) 'Toward publicly auditable secure cloud data storage services', *Network ,IEEE*, vol. 24, no. 4, July, pp. 19-24.