# Security for Cloud Data Protecting by VPN

Ravi Ranjan Kumar
M.Tech CSE
MUR2103922
Department of Computer Science
Mewar University NH 48, Gangarar, Rajasthan 312901

***Abstract*—Context: 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. Aims and Objectives: 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. •**

## 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.**

**Keywords—Challenges, Cloud Computing, Security, Techniques.**

## II. Essential Characteristics of Cloud Computing

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability (pay-per-use basis) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

## III. THREATS FOR CLOUD SERVICE

*A.* Construct validity involves generalizing from your program or measures to the concept of your program or measures. In our research, we have data from Systematic Literature Review (SLR), survey and interviews. Comparison of results from SLR, interviews and survey is hard. We have considered this threat due to inconsistency in data. To overcome this we have used Narrative Analysis for Systematic Literature Review and interview data for proper organization of the data. After receiving the survey data we have thoroughly compared the Narrative Analysis results with the survey results, by this we were able to remove redundancy and inconsistencies in our data.

*B.*

Internal Validity is the approximate truth about inferences regarding cause-effect or causal relationships. There are several problems with conducting survey. One of the major challenges is the redundancy in data interpretation by the practitioners. The redundancy occurs when understanding the question and the answers might be interpreted in another sense which might not be relevant for our work. Based on the understanding of the question her/his answers might differ. To overcome this threat we made sure that the questionnaire is clearly understandable, promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)

*C.* External validity is the degree to which the conclusions in your study would hold for other persons in other places and at other times. The external validity threat of this research describes how well our research conclusions are applicable in general to other related technological areas. In relation to that, the security challenges and techniques of Cloud Computing that we have identified are almost similar to the issues faced in normal traditional network Computing.

## IV. RESULTS AND ANALYSIS

In recent years, the huge amount of research has been done in the area of Cloud Computing. In the process of SLR, we have extracted 69 papers relevant to meet the goals of the research from the large number of papers published since the year 2001. This section covers the results and analysis of the papers that were extracted in the process of SLR. We have given a detailed description of the list of identified challenges and mitigation techniques in appendix section. In the past years, research is followed the distributed computing and mainly focused on service like grid computing. From the last decade, there is a rapid increase in research on new paradigm Cloud Computing which is the next generation computing. We mainly focused on security aspects of the Cloud Computing in last 10 years. Totally 69 papers are retrieved during the literature study. Mostly the selected papers are in between the year 2010 and 2011 which revealed 52 papers and 25 papers respectively. Others include 3 papers published in 2009. The figure below shows the empirical evidence of research on security in Cloud Computing in the last 10 years.

Identified Challenges From the analysis, we have identified 43 security challenges during the SLR. The detailed description of these challenges is presented in Appendix A. The list of identified challenges are WS- security, Phishing attack, Wrapping attack, Injection attack, IP spoofing, Tampering, Repudiation, Information Disclosure, Denial of 30 service, Elevation of privilege, Physical security, WLAN‟s security, Direct attacking method, Replay attack, Man-in-the middle attack, Reflection attack, Interleaving, Timeliness attack, Self adaptive storage resource management, Client monitoring, Lack of trust, Weak SLAs, Perceived lack of reliability, Auditing, Back door, TCP hijacking, Social engineering, Dumpster diving, Password guessing, Trojan horses, Completeness, Roll back attack, Fairness, Data leakage, Computer network attack, Denial of service, Data security, Network security, data locality, Data segregation, Backup, Data integrity, Data manipulation

“In the part of the analysis, we find some of the Cloud Computing attributes which are threats to Cloud Computing. As a part of the result the compromised attributes in Cloud Computing is described in appendix A, they are Confidentiality, Integrity, Availability, Security, Accountability, Usability, Reliability and Auditability. The records of the most threaten attributes are in fig. the fig. shows that Confidentiality 31% and Integrity 24% recorded most threaten, while comparing with usability, reliability, accountability and audit ability which recorded less than the 10%.

Cloud Computing is a new paradigm. Cloud Computing became popular since decade. To find out the security experts in Cloud Computing is complex. In total, we got 16 number of partially and completed responses from the real time survey. However, many do have relevant experience in Cloud Computing and IT security. The adopted experts have experience from 1 to 31 years.

## V .CONCLUSION

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

In the case of some part of local network data placed in the Cloud the security challenges and mitigation techniques were discussed in a Systematic method. Most of the security challenges and techniques that are being used in current Cloud Computing environment are listed in appendix. Few of the popular security techniques that are identified in SLR are Identity based authentication, Service Level Agreement (SLA), Third party auditor, Message authentication codes, Role based access control mechanism, Proof of retrievability, Time bound ticket based authentication scheme. The impact of these security techniques include on Confidentiality, Integrity, Availability and security described in the section 2.4. If you need to exchange sensitive or confidential information between a browser and a web server, Encryption is an obvious tool to protect communication. Proper encryption of data and encryption of transmission is necessary. The mitigation techniques identified from the survey is as follows: • SSL (Secure Socket layer) • VPN (Virtual Private Network) • IPSec (Internet Protocol Security) • A proper use of encryption can give good protection against active attacks. In order to protect against Man-in-the-middle attacks, one should observe if there are any delayed response times, in order to detect if there is any “Middle Man”. • A proper use of encryption can give good protection against eaves dropping. Traffic analysis is harder, but on the other hand, not only that many need protection against this kind of threat.

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

*We have identified the security techniques that are used in the case of when data resides in the Cloud in Systematic process. The identified challenges, mitigation techniques and compromised attributes are described in Appendix section. The few popular security methods are Secure Socket Layer (SSL) Encryption; Multi Tenancy based Access Control, Intrusion Detection System, Novel Cloud dependability model, Hadoop Distributed File System and Hypervisor. From the* Analysis of results from survey we have identified the following security challenges.

## VI. 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.

12. Cong Wang, Qian Wang. (March 2010) 'Privacy Preserving Public Auditing for Data storage security in Cloud Computing', INFOCOM 2010, IEEE, 1-9.

13. Cong Wang, Qian Wang. (2009) 'Ensuring data storage security in Cloud Computing', International Workshop on Quality of Service, 1-9.

14. C. Wohlin. (2000) Experimentation in Software engineering: an introduction, 6th edition, International series in software engineering,Springer.

15. Dawei Sun, Guiran Chang. (Sept.2010) 'A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques', Pervasive Computing Signal Processing and Applications, 305-310.

16. Dawod W, Takouna I. (March 2010) 'Infrastucture as a service security: challenges and solutions', 7th International Conference on Informatics and Systems (INFOS), 1- 8.

17. Doelitzscher F, Reich C. (July 2010) 'Designing Cloud services adhering to Government privacy Laws ', IEEE 10th International Conf. on Computer and Information Technology, 930-935.

18. D.K. Mishra. (Sept.2010) 'Tutorial: Secure Multiparty Computation for Cloud Computing Paradigm by Durgesh Kumar Mishra', Second International Conference on Computational Intelligence, Modelling and Simulation, xxiv-xxv.

19. Ford R.B. (2011) 'Information Security in the Cloud', Network Security, vol. 2011, no. 4, April, pp. 15-17.

20. Gul I, Rehman A. (June 2011) 'Cloud Computing Security Auditing', 2nd International Conference on next Generation Information Technology (ICNIT), 143- 148.

21. Hao Z, Zhong S. (June,2011) 'A Time-Bound Ticket-Base Mutual Authentication Scheme for Cloud Computing', International Journal of Computers, Communications and Control, vol. 6, no. 2, June, pp. 227-235.

22. Huimei Wang, Ming Xian. (May 2011) 'Cloud Evaluation method of Network Attack resitance Ability', Network Computing and Information Security (NCIS), 239-243.

23. Jaatun M.G, Nyre A. A. (March 2011) 'An approach to confidentiality control in the Cloud', Vehicular Technology, Information Theory and Arreospace and Electronic systems Technology, 2nd International Conference on Wireless Communication,1-5.

24. Jensen M, Schwenk J. (Sept.2009) 'On Technical Security Issues in Cloud Computing', IEEE International Conference on Cloud Computing, 109-116.

25. Jia Weiwei Zhu, Haojin Cao. (10-15 April, 2011) 'A Secure data service mechanism in mobile Cloud Computing', Computer Communications Wrokshops (INFOCOMWKSHPS), IEEE Conference 2011, 1060 - 1065.

26. Jin Li, Gansen Zhao. (2010) 'Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing', 2nd International Conference on Cloud Computing Technology and Science, 89-96.

27. Jun Feng, Yu Chen. (Jan 2010) 'Bridging the Missing link of Cloud data storage security in AWS ', 7th IEEE conf. on Consumer Communications and Networking Conference (CCNC), 1-2.

28. Jun Feng, Yu Chen. (Jan 2011) 'Enhancing Cloud storage security against rool- back attacks with a new fais multi party non-repudation protocol', Consumer Communications and Networking Conference (CCNC), IEEE conference 2011, 521- 522.