


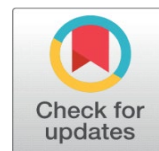
CONCEPTUAL MODEL DEPICTING RISK FACTORS INFLUENZING CLOUD DATA SECURITY



Remya Nair ¹✉, Dr. J. Meenakumari ²✉ 

¹ Research Scholar (Registered with University of Mysore), Bangalore, India.

² Professor & HOD Research, ISME, Bangalore, India.



ABSTRACT

Cloud Platform has the data stored in a remote server and accessed with the help of services provided by cloud service providers. The primary objective is to provide data security due to the confidentiality of data transmitted to the remote server, over an unmonitored and multi-tenancy channel (internet). The major components of cloud platform are application, service, runtime cloud, storage and infrastructure. This is a conceptual paper trying to explain the risk factors to be deemed in a cloud environment. The benefits include scalability, availability, reliability, flexibility, increased collaboration, competitive edge, sustainability, reduced proportional cost. Risk factors influencing the data security and Integrity are identified up to three level of sub-constructs. All the risk factors including hackers, mishandling of passwords, risk of data accessed from public /unmonitored sources, security in communication channels, intentional and unintentional data security threats created due to human interference are included in the scope of this paper. In this paper, the identification of sub factors of cloud data security risk components is achieved. The futuristics scope of this paper is to identify early risk prediction and mitigation strategies to all the identified risk factors related to data security by implementing SEM methodology.

Keywords: Cloud Data Security, Risk Factors, Human Intervention, Conceptual Model, Data Privacy, Architectural and Design Flows

Received 28 July 2021
Accepted 12 August 2021
Published 31 August 2021

Corresponding Author

Dr. J. Meenakumari,
meenakumari@isme.in

DOI
[10.29121/granthaalayah.v9.i8.2021.4160](https://doi.org/10.29121/granthaalayah.v9.i8.2021.4160)

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2021 The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

1. INTRODUCTION

The term “cloud” refers to a distinct Information Technology environment, specifically designed for remotely provisioning scalable, reliable and measurable IT resources. An IT resource is a physical or virtual IT artifact that can be software based (virtual server, custom software program) or hardware based (physical server, network device). The major application-based advantages of cloud computing are

- **Cloud Big Data Analytics:** will assist in progressive and insightful customer relationships
- **Cloud Business Models:** deals with development of innovative cloud business models to satisfy advanced objectives
- **Cloud Decision Support Systems:** will ensure smooth processing of complex business data analysis
- **Business Process and Cloud Consulting:** will ensure competitive Advantage from Cloud Computing by implementing advanced business process and better consulting options
- **Cloud Business Collaboration:** will provide efficient and effective tools for



business workers.

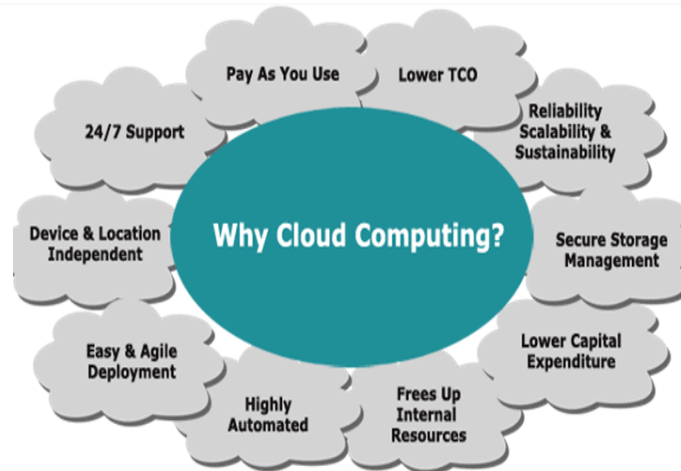


Image courtesy(<https://consoleradius.com/why-cloud-computing/>)

2. BENEFITS OF CLOUD COMPUTING

Some of the benefits of Cloud computing are unlimited storage capacity, multi-tenancy, high speed, quick deployment, fast and effective virtualization location and device independence etc. The key features of these benefits are the following

Scalability: Cloud scalability refers to the potential to dynamically increase or decrease the IT resources based on the demand. Scalability is the primary driver of cloud's exploding popularity.

Availability: In the context of cloud computing, availability is the duration the service provider guarantees that data and services are accessible. There are systems that cannot tolerate interruption in service as well as where downtime can cause damage or financial loss. Ensuring available in such critical systems is inevitable.

Reliability: The reliability of cloud system is the duration for which the desired functions are performed uninterruptedly without failure.

Flexibility: The files can be accessed using web-enabled devices such as pc, smartphones, laptops etc. The capability to concurrently share files and data over the Internet can also facilitate both internal and external collaboration.

Increased Collaboration: The fundamental advantage of collaboration is the capability to share knowledge and expertise promptly and effortlessly. In cloud collaboration, many individuals can access, review and edit a document in real time. The advantage of document housed in the cloud is that it is always versioning. Hence everyone with access can see the changes as and when they are made. The advantage of cloud collaboration is that the efforts of combining multiple documents and wrestling with outdated versions have become a thing of the past.

Competitive Edge: Enhanced customer relationships driven by big data analytics, precise business decision making from cloud decision support systems, and enhanced business collaborations are the competitive advantages of using cloud computing.

Sustainability: Sustainability in cloud, positions IT companies to deliver on new obligations: carbon reduction and responsible innovation. The IT companies have traditionally driven financial, security, and agility benefits through cloud, but sustainability is becoming a necessity.

Reduced Proportional Cost: In cloud computing, pooled IT resources are accessible and shared by numerous cloud consumers, resulting in improved or maximum possible utilization. Operational costs and inefficiencies can be further reduced by better management and governance, implementing verified practices and patterns for optimizing cloud architectures.

3. THEORETICAL BACKGROUND (LITERATURE REVIEW)

In Cloud Platform neither the exact location of the data nor the other sources of the data jointly stored will be known to the user. The data found in cloud ranges from public source (which has negligible security concerns) to private data containing extremely sensitive information (such as social security numbers, medical records, or shipping manifests for hazardous material) (L. M. Kaufman, 2009) [Khorshed et al. \(2012\)](#) Cloud Computing trends like Grid Computing, Utility Computing, Distributed Computing are rapidly advancing. Cloud service providers such as Amazon IBM, Google's Application, Microsoft Azure etc., aid in developing applications in cloud environment and help users to access them from anywhere. Cloud data, is generally stored in a remote server and accessed with the help of services provided by cloud service providers. The major concern is providing security as the confidentiality of the data transmitted to the remote server over a channel (internet) has to be maintained. The priority is to address the security challenges before implementing Cloud Computing in an organization [Rao and Selvamani \(2015\)](#). Multi tenancy is one of the major factors which should be taken into account while considering the data security risks (Hussain AlJahdali et al, 2014) [Vaquero et al. \(2008\)](#)

L. M. Kaufman, "Data Security in the World of Cloud Computing" [Khorshed et al. \[1\]](#)- This paper implies on the fact that if a cybercriminal can identify the provider whose vulnerabilities are the easiest to exploit, then the particular cloud setup becomes a highly visible target. The identified gaps are that the paper covers the data security risks on a high level and it has not considered individual factors.

H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau and J. Xu, "Multi-tenancy in Cloud Computing," [AlJahdali et al. \(2014\)](#) this paper covers the Multi-tenancy in Cloud Computing. Case1: internet attacks Case2: Attacks within cloud provider Case3: multi-tenancy attacks. Multi- tenancy advantages and risks and partial attack model is in the scope of this paper. All the other risk factors are not taken into consideration in this paper.

[Rao and Selvamani \(2015\)](#) in the paper "Data Security Challenges and Its Solutions in Cloud Computing" implies that Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. The identified gap is that First level data security challenges are identified and solution is provided. However, in-dept analysis of each of the factors and solutioning detail is lacking in the paper.

[Subashini and Kavitha \(2011\)](#). "A survey on security issues in service delivery models of cloud computing" *Journal of Network and Computer Applications*, 34(1), 1-11 explains all the three components of Cloud. The 3 components IaaS, PaaS and

SaaS is considered for all the risk factors Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization. Data confidentiality, Web application security, Data breaches, virtualization vulnerability, Availability, Backup, Identity management and sign-on process Although all the components of cloud are considered, the data risk factors are classified at only one level of constructs and the root cause that led to all the risk factors is not evaluated in-depth.

Dimitrios Zissis, and Dimitrios Lekkas, "Addressing cloud computing security issues," [Zissis and Lekkas \(2012\)](#) explain in the paper Cloud platform is analysed in application level, virtual level, physical level. Users of each level and security requirements are identified. The first level of security threats in each of these identified requirements is explained. However, second and third level of construct or rather analysis of root cause of these security threats is not present in this paper.

In this paper by Chonka, A, Xiang, Y, Zhou, W, and Bonti, A (2011) "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks" [Chonka et al. \(2011\)](#), Cloud Protector, a neural network is developed that was trained to detect and filter X-DoS attack in this paper Cloud Protector, a neural network is developed that was trained to detect and filter X-DoS attack. This paper concentrates only on the exogenous risk factor, the threat due to attacks. The other data security risks other than an explicit attack is not taken into consideration.

In the paper by Jansen, W. A. (2011) Cloud Hooks: Security and Privacy Issues in Cloud Computing [Jansen W. A. \(2011\)](#) primary level risk factors are considered. However in-depth risk analysis of each of these risk factors and weightage of each parameter is not taken into account.

Three main goals of the paper by Md. Tanzim Khorshed, A.B.M. Shawkat Ali, and Saleh A.Wasimi, "A Survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," [Khorshed et al. \(2012\)](#) are: (i) to detect an attack when it happens, (ii) to inform related parties (system admin, data owner) about the attack type and take combating action, and (iii) to create information on the type of attack by analysing the pattern The sub factors that contribute to risk or threats are not considered in this paper. This paper presents a holistic approach towards the identification of proactive risk mitigation.

4. THEORETICAL FINDINGS – RELEVANCE OF THIS PAPER

As part of the theoretical reviews all the above discussed papers have macrolevel perception of the data security risks. In-depth multilevel analysis is not covered in any of these papers. As per the interviews with experts and professional discussions with practitioners, to strategize the early risk predictions understanding of the root cause or the basic parameters that contribute the risk is important. This paper targets to fill the gaps by identifying up to three level of constructs to trace the root cause of the cloud data security risk factors.

5. OBJECTIVES OF THIS PAPER

The objectives of this paper are

- 1) Identify the parameters that contribute to the risks in cloud data security
- 2) Group them under proper classification

- 3) Ensure the relevance of subfactors in each group
- 4) Theoretically ensure that all the areas of risk factors in cloud data security are covered

6. METHODOLOGY

This is a qualitative and conceptual paper. The basic purpose of this paper is to identify the risk factors in cloud data security implementing descriptive study. Up to three levels of subconstructs of the risk factors in data security are identified. The ideas and factors were gathered from the literature review. Interviews of experts and professional discussions with practitioners also formed the background for this paper. The in-depth analysis on the factors were basically obtained during the professional discussions with a few practitioners working in this realm.

7. IDENTIFICATION OF RISK FACTORS

Based on the literature reviews, expert interviews and professional discussions with practitioners the risk factors are identified. The data in cloud is generally stored in a remote server and accessed with the help of services provided by cloud service providers. The risk could be due to both exogenous and endogenous risk factors the primary concern is to provide data security as the confidential data is transmitted to the remote server over an unmonitored and multi-tenancy channel (internet). The primary constructs in Cloud Data Security are

- Architecture/ Design Flows in the system
- Human Intervention
- Access risks from unprotected sources
- Data privacy
- Password security

Architecture/ Design Flows in the system

The basic architecture or design of the cloud system must be planned with at most clarity and precision. The subconstructs that contribute to the risk parameters of architecture of a cloud system are planned risks not handled, risk tracking not in place/ not effective, risk mitigation not planned effectively, changes in subsystems, unplanned risks.

Risk factors due to human intervention

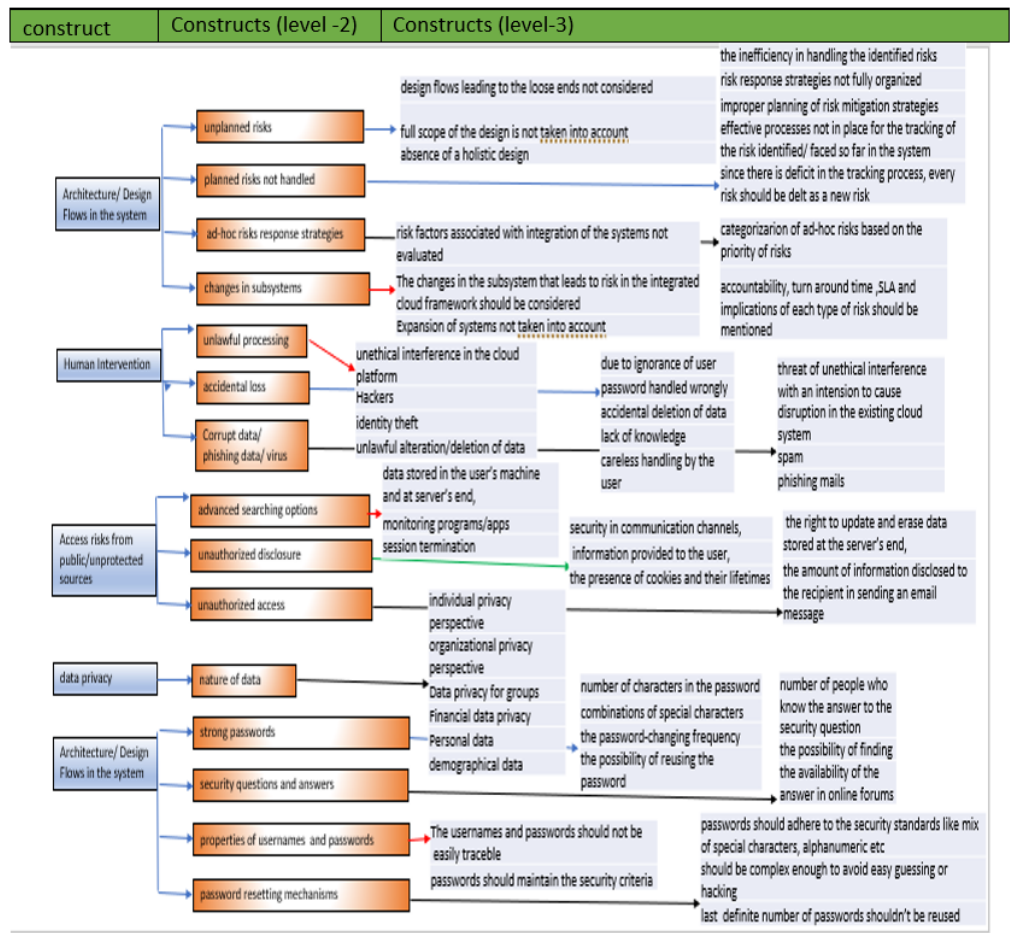
The human interactions are a major contribution to the risks involved in a cloud environment.

The major human made errors could be categorized into two sections. Intentionally created threats/risks and the risks created unintentionally. The intentionally created risks include the unlawful processing comprising of the Hackers, identity theft, unlawful alteration/deletion of data. The unintentional or accidental risk factors due to human intervention includes password handled wrongly, accidental deletion of data, lack of knowledge. The phishing data and viruses are a serious threat to the risk handling efforts in Cloud Platform. Spam and phishing mails pose a serious threat to the data security and integrity.

Access risks from public/unprotected sources

The access of data from unprotected sources is a serious data security issue faced by the Cloud Platform. Data stored in the user’s machine and at server’s end could be easily compromised by advanced searching options. The unmonitored programs/apps as well as the improper session terminations could result in data security risks. Unauthorized disclosure of information, security in communication channels, information provided to the user, the presence of cookies and their lifetimes all add to the data security risks. Unauthorized access, the right to update and erase data stored at the server’s end, the amount of information disclosed to the recipient in sending an email message all are contributing parameters that increase the data security risks.

A table depicting the second and third level constructs of each factor are as follows (Figure 3)



Data privacy

The confidentiality and integrity of data handled manifolds the data security risks. Individual privacy perspective, organizational privacy perspective, data privacy for groups, personal data as well as demographic data all add on to the data security risks. The most confidential and protected data in cloud is the financial data.

Password security

The primary factor to be considered in data security maintenance is the password security. Strong passwords comprising of number of characters in the password, combinations of special characters, the password-changing frequency as well as the limited possibility of reusing the password should be ensured. The following parameters like number of people who know the answer to the security question, the possibility of finding it and the availability of the answer in online forums must be considered while implanting the security questions and answers. The properties of usernames and passwords as well as the security of password resetting mechanisms should be ensured.

8. EXPLICIT CONTRIBUTION

The literature reviews have revealed the gaps in the standing papers and identified the sub factors or subconstructs that should be considered while evaluating the data security risks in cloud. The second and third level of constructs identified as per figure 3 are the root causes or the sub-parameters that contribute to the risk factor. The evaluation has to be done for these sub parameters to estimate their contribution to overall risk in the cloud platform. The subconstructs identified with the help of interview of experts and discussions with practitioners and considering practitioner suggestions caters as the initial foundation for the SEM Methodology interpretation of the risk factors in cloud, which is the futuristic scope of this paper.

9. CONCLUSION

Cloud Platform provides an effective, optimized, scalable data storage and processing option that could be accessed from anywhere. However due to multi-tenancy and other factors the risk with the cloud data is multi folded. A multi-tenancy in cloud computing architecture allows customers to share IT resources in a public or private cloud. However, the data security is the primary concern in cloud. The main parameters in cloud data protection are confidentiality, availability, reliability and integrity. Impact due to any data mishandling or data manipulation is huge in case of a cloud platform due to the size, complexity and confidentiality of the data stored. In this paper, the risk factors influencing the cloud data security is identified. The gaps identified from the other papers, which is the identification of sub constructs in each of these risk factors is addressed in this paper. The futuristic scope of this paper is to evaluate the contribution of sub parameters to overall data security risk as well as to formulate the early risk prediction plan for each of these identified and evaluated parameters incorporating SEM methodology.

REFERENCES

- Aljahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., & Xu, J. (2014). Multi-tenancy in Cloud Computing. 2014 IEEE 8th International Symposium on Service Oriented System Engineering. Retrived from <https://doi.org/10.1109/SOSE.2014.50>

- Chonka, A., Xiang, Y., Zhou, W., & Bonti, A. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*, 34(4), 1097-1107. Retrived from <https://doi.org/10.1016/j.jnca.2010.06.004>
- G. Xu, H. Li, H. Ren, K. Yang and R. H. Deng (2019), "Data Security Issues in Deep Learning : Attacks, Countermeasures, and Opportunities," in *IEEE Communications Magazine*, vol. 57, no. 11, pp. 116-122, November, Retrived from <https://doi.org/10.1109/MCOM.001.1900091>
- Gheyas, I.A., Abdallah, A.E. (2016) Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Anal* 1, 6. Retrived from <https://doi.org/10.1186/s41044-016-0006-0>
- Hoyle, R. H. (Ed.). (1995). *Structural equation modeling : Concepts, issues, and applications*. Sage Publications, Inc.
- Jansen, W. A. (2011). *Cloud Hooks: Security and Privacy Issues in Cloud Computing*. 2011 44th Hawaii International Conference on System Sciences. Retrived from <https://doi.org/10.1109/HICSS.2011.103>
- Kaufman, L. M. (2009). *Data Security in the World of Cloud Computing*. *IEEE Security & Privacy Magazine*, 7(4), 61-64. Retrived from <https://doi.org/10.1109/MSP.2009.87>
- Khorshed, M. T., Ali, A. B. M. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, 28(6), 833-851. Retrived from <https://doi.org/10.1016/j.future.2012.01.006>
- L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. (2008) A break in the clouds: towards a cloud definition, in: *ACM SIGCOMM Computer Communication Review*, p.50-55. Retrived from <https://doi.org/10.1145/1496091.1496100>
- M.B. Mollah, K.R. Islam, and S.S. Islam. (2012) Next generation of computing through cloud computing technology, in : 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6. Retrived from <https://doi.org/10.1109/CCECE.2012.6334973>
- MacCallum, R. C., & Austin, J. T. (2000). Applications of structural equation modeling in psychological research. *Annual Review of Psychology*, 51, 201-226. Retrived from <https://doi.org/10.1146/annurev.psych.51.1.201>
- Olusola Akinrolabu, Jason R.C. Nurse, Andrew Martin, Steve New (2019), Cyber risk assessment in cloud provider environments: Current models and future needs, *Computers & Security*, Volume 87 ,101600,ISSN 0167-4048, Retrived from <https://doi.org/10.1016/j.cose.2019.101600>
- Pragati Priyadarshinee, Rakesh D. Raut, Manoj Kumar Jha, Bhaskar B. Gardas, (2017) Understanding and predicting the determinants of cloud computing adoption : A two staged hybrid SEM - Neural networks approach, *Computers in Human Behavior*, Volume 76, Pages 341-362,ISSN 0747-5632, Retrived from <https://doi.org/10.1016/j.chb.2017.07.027>.
- Rao, R. V., & Selvamani, K. (2015). *Data Security Challenges and Its Solutions in Cloud Computing*. *Procedia Computer Science*, 48, 204-209. Retrived from <https://doi.org/10.1016/j.procs.2015.04.171>

- Rigdon, E. E. (1998). Structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 251-294). Lawrence Erlbaum Associates Publishers.
- Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou (2010). Achieving secure, scalable and fine-grained data access control in cloud computing, in: *IN-FOCOM, Proceedings IEEE*, 2010.p.1-9.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11. Retrived from <https://doi.org/10.1016/j.jnca.2010.07.006>
- X. Zhang, N. Wuwong, H. Li and X. Zhang (2010), "Information Security Risk Management Framework for the Cloud Computing Environments," 2010 10th IEEE International Conference on Computer and Information Technology, pp. 1328-1334, Retrived from <https://doi.org/10.1109/CIT.2010.501>
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592. Retrived from <https://doi.org/10.1016/j.future.2010.12.006>.