www.ijarp.com ISSN 2456-9992 Page: 01-08

Review Article

International Journal Advanced Research Publications

Volume: 02
Issue: 10

A REVIEW OF DATA SECURITY CHALLENGES AND SOLUTIONS IN CLOUD COMPUTING

J. Shalini Devi*[1], J. Roselin[2], M. Asha[3]

M.Com Computer Applications

[1,2,3]Department of Commerce Computer Applications, St. Joseph's College (Autonomous), Tiruchirappalli, India.

Article Received: 11 September 2026, Article Revised: 01 October 2026, Published on: 21 October 2026

***Corresponding Author: J. Shalini Devi**

M.Com Computer Applications Department of Commerce Computer Applications, St. Joseph's College (Autonomous), Tiruchirappalli, India.

Doi: https://doi-doi.org/101555/ijarp.8500

ABSTRACT

Cloud computing is technology developing demand architecture, which was really useful for IT enterprises. Using cloud computing that offers cost effective & customer flexible service. This cloud computing is useful for big organization like Google, Facebook, Dropbox etc. And also this may increase the competence of the organization without giving new training for the fresher. Various countries data centers adopting cloud computing because of its database and application but the highest priority is for the securing of data. Cloud computing is Mainly used for its performance, accessibility and its affordable price. The main purpose of using cloud computing is for the protection of data. When we aware the word data security means the first thing is qualities (confidentiality, integrity and availability). In this data security is also having major issues, which means the data stored that was automatically stored over the cloud. When we used to see the development of computing technology in the cloud environment for the future advancement is fully based on the data privacy and data security protection. It may helps to use mainly for the organization & government sector.In this paper discussed about cloud computing security challenges and issue, while transferring the data into the cloud and also get reliable solution to overcome from the data security while using the cloud environment. That the comparative research from the existing cloud security approach about data privacy and data security by utilizing cloud computing. It will be useful to strengthen the security of data storage in a cloud environment.

KEYWORDS: Data security, Data locality, Data integrity, Data Security issues.

1. INTRODUCTION

In this dynamic environment developing technologylike cloud computing play vital role to reach globally abecause of itslow cost and powerful way of working and satisfying their user needs[1][2]. Technology developing is going rapidly that's why it introduced Cloud computing, these can be use or owned by both organization as well as common people based on their demand[3][4]. For storing and managing of large data securely means the choice is always move to cloud computing[5]. User wants to store their data in a secure way they can store it into cloud service[6]. The cloud services are Infrastructure as a service (IAAS), Platform as a service (PAAS), and Software as a service (SAAS)[7][8].

In the previous years, fast access gaining and cloud resources where increasingly accommodate by different business organization, through this they can overcome from the issue of paying initial cost for the resources they used[9]. Developing software like Microsoft, Google, Amazon, IBM where using cloud computing for its advantage but there is also an issue of storing data[10][11]. Data security has a problem in cloud computing environment because of its storage issues.In the era of cloud computing Data privacy and security are the two main aspects in cloud computing environment for its issues like privacy, data confidentiality, integrity[12][13]. Because user's data are stored on servers which is managed by third-party providers, there is a high risk of unauthorized access, data leakage, and privacy violations[14]. There is aavailability of data risk misuse when numerous organizations share resources or data. Without proper security mechanisms, data stored in cloud systems gone through attacks including data theft, insider threats and unauthorized access[15].

Therefore, maintaining users trust and the reliability of cloud services requires strong protection mechanisms. Encryption is one widely used for protecting data in cloud environments. Encryption is powerful methods for securing sensitive data in cloud computing environment. Encryption methods turnreadable text into cipher text through encryption becomes Unreadable and can be accessed only by authorized parties with the proper key to decrypt it.[16]

2. Literature Review

The study start by identifying the security challenges of transferring and storing of data in the cloud.Cloud computing refers to the delivery of on-demand resources instead of owning and

maintaining its infrastructure. However, it provides major benefits through its services, but there are security challenges and issues remain in the cloud computing environment. The primary purpose of the researcher is to secure sensitivity data stored in the cloud. Muhammad Abrar Rayhan reviewed that encryption techniques are efficientway for enhancing data security and also mentioned security issues and challenges related to data such as VM attacks, loss of governance, Data leakage[17]. Abubakar Jibrin and Aliyusani Ahmad conducts a multilevel assessment on enhancing security related to data in cloud computing environment[18]. Finally, JR. Ancyjero elaborates about data breaches and insider threat in an organization. Collectively, these studies talk about the significance off cryptographic techniques, setting clear boundaries to address the challenges and issues of data security in cloud computing[19]. Merging of these approaches will absolutely improve confidentiality, integrity and Availability of data in cloud environment[20][21].

Securing of data is dependent on the state of the data and the environment which means Protecting information in cyberspace, using cloud systems, and employing encryption mechanisms[22][23]. Encryption in the term converting plaintext into ciphertext through this the unauthorized person can't able to attack[24][25]. This approach provides more security for data transmission and authentication[26][27]. Researchers of data security in cloud computing suggested that the different encryption techniques could add a new level of security to cloud computing [28][29].

3. Problem Definition

Cloud computing has become an essential technology for storing, managing, and accessing data over the internet. Despite its numerous advantages, security concerns remain a major obstacle to its widespread adoption. Data stored in cloud environments may be exposed to various threats, including unauthorized access, data breaches, malicious attacks, insider threats, and improper access control. Since users have limited direct control over data stored on third-party cloud servers, ensuring data confidentiality and privacy becomes a significant challenge. Traditional security mechanisms may also introduce additional computational overhead, processing delays, and storage costs. Therefore, there is a need for an effective and cost-efficient security mechanism that protects sensitive data in cloud environments while minimizing encryption and decryption time and resource consumption. Addressing these challenges is essential to improve data security, strengthen user trust, and promote the reliable adoption of cloud computing.

4. Categories of Enhancing Data Security in Cloud Computing

Data security in cloud computing is totally based on cloud service provider (CSP). The issues related to data are security, locality, Integrity, Segregation, Access.

(A) Data security: A risk of data misuse, it is required to secure data storage, process or transit. It is the most important challenge among other cloud computing challenges.

(B) Data locality: "Does CSP allow to control the data location?" Necessary that customer should be inform about the location of the data stored.

(C) Data integrity: Data integrity must be maintained correctly, when database are in multiple locations.

(D) Data segregation: Multi-tenancy leads to data intrusion of clients & users. They should ensure data should separate from other users.

(E) Data Access: Data accessed by employees, it may be partial data and complete data access. They should ensure which data is accessed by which employee.

5. Proposed Solutions for Enhancing Data Security in Cloud Computing

The security challenges in cloud computing can be addressed by implementing effective security techniques to protect sensitive data from unauthorized access, modification, and misuse. The proposed solutions focus on improving data confidentiality, integrity, access control, and secure data storage. The following techniques can be adopted to enhance data security in cloud environments.

i. Encryption Techniques: Encrypt sensitive data before uploading it to the cloud. This ensures that unauthorized users cannot understand the data even if they gain access to the stored files.

ii. Data Location Management: Select cloud service providers that clearly disclose data storage locations and comply with applicable data protection regulations.

iii. Data Integrity Verification: Use hashing algorithms and digital signatures to verify that stored data has not been modified without authorization.

iv. Data Segregation: Apply tenant isolation, separate encryption keys, and secure storage configurations to prevent data leakage between different cloud customers.

v. Access Control Mechanisms: Implement role-based access control (RBAC) and multi-factor authentication to ensure that only authorized users can access sensitive information.

vi. Regular Monitoring and Auditing: Monitor user activities, review access permissions, and conduct regular security audits to identify suspicious activities and potential vulnerabilities.

vii. Efficient Security Mechanisms: Develop security techniques that reduce encryption and decryption time while maintaining strong data protection and minimizing computational overhead.

CONCLUSION

In this digitalized era, cloud computing is an emerging technology that offers numerous benefits to its users. However, its adoption is sometimes hindered by data security issues and challenges. This study helps to understand and analyze the vulnerabilities and security issues associated with cloud computing. Among these challenges, data security is one of the most crucial concerns, as the data stored in the cloud may contain highly confidential and sensitive information. Therefore, enhancing data security in cloud environments is essential to ensure data confidentiality, integrity, and availability while building user trust and confidence. Implementing effective security measures, such as data encryption, strong access control mechanisms, authentication techniques, and continuous security monitoring, can help minimize security risks and protect sensitive information from unauthorized access and potential cyberattacks. By addressing these challenges and adopting reliable security practices, cloud computing can become a more secure, trustworthy, and efficient technology, thereby encouraging wider adoption among individuals and organizations.

REFERENCES

1. Juare, S, “Survey on Data Security and Integrity Issues in Cloud Computing”,IOSR Journal of Computer Engineering, 2016, pp. 59-62.
2. Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., &Deris, M. M, “A Survey on the cryptographic encryption algorithms”, International Journal of Advanced Computer Science and Applications, 2017,pp.333-344.
3. ManishaKumari, Kirubanad V.B,“Data encryption and decryption using graph plotting. International Journal of Civil Engineering and Technology”, 2018, pp.36-46.
4. Kalpana, G., Kumar, P. V., Aljawarneh, S., & Krishnaiah, R. V,“Shifted adaption homomorphism encryption for mobile and cloud learning”, Computers & Electrical Engineering,2018,pp.178-195.

5. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N,"Hybrid optimization with cryptography encryption for medical image security in Internet of Things", Neural computing and applications,2018, pp. 1-15.
6. Yang, L., Han, Z., Huang, Z., & Ma, J, "A remotely keyed file encryption scheme under mobile cloud computing. Journal of Network and Computer Applications", 2018, pp. 90-99.
7. Al Badawi, A. Q. A., Polyakov, Y., Aung, K. M. M., Veeravalli, B., & Rohloff, K. "Implementation and performance evaluation of RNS variants of the BFV homomorphic encryption scheme", IEEE Transactions on Emerging Topics in Computing, 2019.
8. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B, "Secure integration of IOT and cloud computing, Future Generation Computer Systems", 2018, pp.964-975.
9. Shanthni, K. K., Kaviya, K., Sujithra, M," A Survey on Cloud Computing: Data Security Challenges and Their Defensive Mechanisms", International Journal of Recent Science, 2018, pp.26497-26500.
10. Dr. D. I. George Amalarethinam, B.Fathimamary, "DMUCE- A Confidentiality Enabled Technique To Improve Cloud User Security", International Journal of Applied Engineering Research,2015, pp.34103-34108.
11. Dr. D. I. George Amalarethinam, B.Fathimamary, "eDSSuMRT- Ensured Data Security Strategy using Matrix Random Traversal In Cloud Storage Environment", International Journal of Applied Engineering Research,2015,pp.272-279.
12. Dr. D. I. George Amalarethinam, B.Fathimamary, Confidentiality Technique for Enhancing Data Security in Public Cloud Storage using Data Obfuscation, International journal of control theory and application,2016,pp.1-11.
13. Dr. D. I. George Amalarethinam, B.Fathimamary, Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography, IEEE Explore,2016, pp.181-184.
14. B. Fathimamary, Dr.D.I George Amalarethinam, Data security enhancement in public cloud storage using data obfuscation and steganography, world congress on computing and communication technologies (WCCCT),2016, pp.181-184.
15. Dr. D. I. George Amalarethinam, B.Fathimamary, Data Security Enhancement in Public Cloud Storage, Journal of Computing and Intelligent Systems, 2017, pp.1-5.
16. Dr. D. I. George Amalarethinam, B.Fathimamary, Security Enhancement for Public Cloud Storage with Minimum Cost, International Journal of Pure and Applied Mathematics,2018, pp.1-9.

17. Rayhan, M. A., “Enhancing Data Security in Cloud Computing Using Encryption Techniques”, 2026. DOI: 10.5281/zenodo.18908828.
18. Jibrin, A., and Ahmad, A. S., “Enhancing Security in Cloud Computing Environment”, Advanced Journal of Science, Technology and Engineering, vol. 6, issue 1, 2026, pp. 28–40. DOI: 10.52589/AJSTE-BUIU5R07.
19. Ancy Jero, J. R., and Misbha, D. S., “Data Security and Cloud Computing Environment”, Conference Paper, De Paul Degree College, Mysore, 2026.
20. Dr.D.I.George Amalarethinam, B.Fathimamary, “Comparative Analysis of Obfuscation Techniques in Public Cloud”, American International Journal of Research in Science, Technology, Engineering & Mathematics,2019,pp.309-312.
21. Halevi, S., Polyakov, Y, Shoup V, “An improved RNS variant of the BFV homomorphic encryption scheme in Cryptographers”, Springer, pp. 83-105.
22. Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S, “A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing”, International Journal of Intelligent Networks, 2022, pp.16–30. https://doi.org/10.1016/j.ijin.2022.04.001
23. B Fathimamary, “Data Security Enhancement In Cloud Using Magic Square Obfuscation”, International Multidisciplinary Research Journal Reviews (IMRJR), vol.2, 2025, pp.66-70. https://DOI: 10.17148/IMRJR.2025.020908
24. B Fathimamary, “A Comprehensive Study on Cryptographic Approaches for Securing Data in Cloud Storage”, International Multidisciplinary Research Journal Reviews (IMRJR), vol.2, Issue 11, 2025, pp.66-72. https:// DOI: 10.17148/IMRJR.2025.021107
25. B Fathimamary, A novel magical encryption technique for secure and efficient public cloud storage. Advancement of Computer Technology and Its Applications. 2026; vol. 9, Issue 2, pp.45-50. https://doi.org/10.5281/zenodo.18397099
26. B Fathimamary, Baby Nirmala M, Nasreen M. Enhanced Positional Vigenère (EPV): A confidentiality enabled encryption technique for secure cloud storage. The Scientific Temper, vol.17, issue 4, pp.6005-6009. https://doi.org/10.58414/SCIENTIFICTEMPER.2026.17.4.09
27. B Fathimamary, Rexy J, Geetha R, “A Novel Three-Layered Security Framework for Enhancing Data Confidentiality in Cloud Storage Environments”, Indian Journal of Science and Technology. vol.19, issue 31, 2025, pp.2197-2205. https://doi.org/10.17485/IJST/v19i31.1093

28. B Fathimamary, “An Efficient DDoS Attack Detection Using Optimized Long Short-Term Optimization Based on Improved Brainstorm Optimization”, Indian Journal of Science and Technology vol.19, Issue 5, 2026, pp.298–312. https://doi.org/ 10.17485/IJST/v19i5.2020
29. B Fathimamary, “An ASCII-Based Matrix Technique for Enhancing Data Confidentiality in Cloud Computing”, International Multidisciplinary Research Journal Reviews (IMRJR), vol.3, issue 10,2026,pp.15-19. DOI 10.17148/IMRJR.2026.031004.