International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

# A PAPER ON

# DATA SECURITY IN CLOUD COMPUTING

**Alok Katiyar[1], Atul Pratap Singh[2], Anshuman Singh[3], Anuj Pratap Singh[4], Pranjal[5]**

*[1]Assistant Professor, Department of Computer Science & Engineering, Inderprastha Engineering College, Ghaziabad, Uttar Pradesh, India*

*[2,3,4,5] Students, Department of Computer Science & Engineering, Inderprastha Engineering College, Ghaziabad, Uttar Pradesh, India*

---

**ABSTRACT**

Cloud computing is the service that can be accessed by the Internet and the next stage evolution of the Internet. In this, we can get facilities anytime on-demand by the cloud providers to store information without active management of the users **[11]**, in the last few years. We can see an increase in the use of cloud technology, but cloud security is even a significant issue because even many firms are not using the cloud. In this, client data is put away at different data communities distributed at various areas on the planet, and the client doesn't have the foggiest idea where his/her information is put away on the earth **[9][5]**. There are many security problems in cloud computing and need to resolve for the growth of cloud computing. There are many concerns about information security because the user has no control over it and stored it in the providers' premises. In our study, we attempt to review the research in this field **[8].**

**KEYWORDS**

**Information security, Information concealer, Denial of facilities, Cloud information, Concealment**

## 1. INTRODUCTION

Cloud computing viewed as the next-generation paradigm in integration. Cloud is a hardware and software environment in information centers that provide multiple facilities on the network or the Internet to satisfy user needs. The definition of "cloud computing" from the National Institute of Standards and Technology (NIST) is that cloud computing offers access to, secure, required networks in a shared pool of computational resources (e.g., networks, servers, storage, systems apps, and facilities). According to the definition, cloud computing offers secure access to the search network in a shared pool of computational resources. Resources refer to computer resources, network resources, platforms, software resources, virtual servers, and computer infrastructure **[2] [19].**

Data scientists can consider cloud computing as a new computing arc that offers facilities on-demand at minimal costs. The three most popular and commonly used service models in the cloud example are Software One Service (SaaS), Platform One Service (PaaS) Infrastructure One Service (IAS).

SaaS implements software with relevant information. Users can access it through cloud service providers and a web browser.

In PaaS, service providers facilitate users with a set of software programs that can solve specific tasks. At IaaS, cloud service providers offer customers with virtual machines and storage to improve their business capabilities. Cloud computing is closely related but not the same as grid computing. Grid computing interconnects multiple resources and controls sources with integrated managing systems to provide high-performance computing facilities.

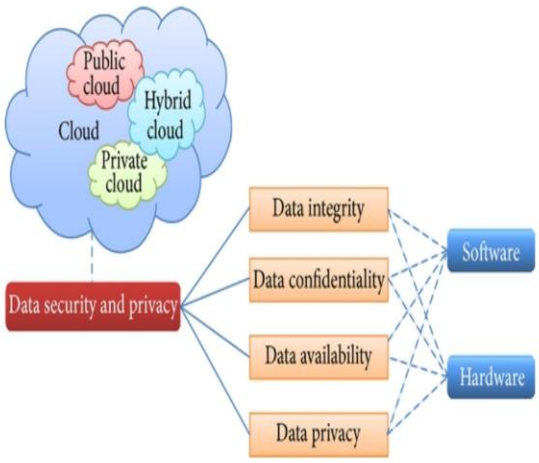
In contrast, cloud computing offers a variety of managing facilities to impart significant information storage and high-performance computing, combining computing and storage resources managed by systems. Multiple researchers analyzed the privacy and information security issues in cloud computing

by focusing on privacy, information sharing, and cloud security. Information security issues are mainly at the SPI (SaaS, PaaS, and IaaS) level, and the main challenge in cloud computing is information sharing. In this paper, we review multiple security techniques and problems for information storage security and privacy protection in cloud computing environments **[3] [17] [32].**

As Figure 1 shows, this paper presents a similar research investigation existing research on techniques used in cloud computing through information security issues, including information integrity, privacy, and availability.

Information privacy issues and methods are studied virtually in the cloud, as information privacy is traditionally associated with information security. Comparative studies on information security and privacy can help increase user confidence by getting information in a cloud computing environment. **[7] [22]**

**Image (a): Information Security and Privacy[41]**




## 2. INFORMATION INTEGRITY

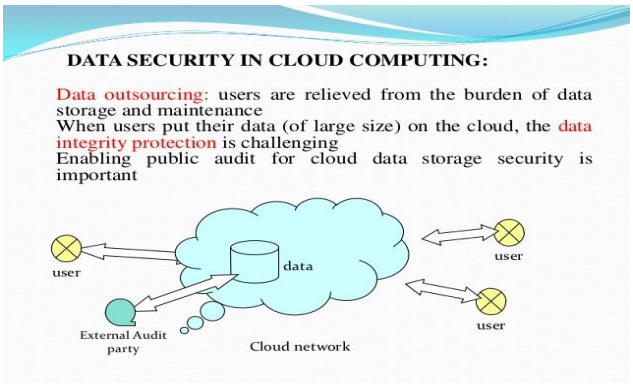
Information integrity is one of the most critical aspects of any information system. Generally, information integrity means protecting information from unauthorized removal, modification, or creation. Maintaining the company's access to and rights to specific enterprise resources ensures that valuable information and facilities are misused, misused, or stolen.

Transactions must adhere to acidity (atomicity, consistency, isolation, and durability) characteristics to ensure information integrity. Most information bases support ACID transactions and maintain information integrity. Authorization used to control access to information. The system determines the level at which a particular user has access to secure resources managed by the system **[33].**

Cloud computing providers are trusted to maintain information integrity and accuracy. However, it is necessary to build a third-party monitoring mechanism along with customers and cloud service providers. Remotely verifying the integrity of information in the cloud is a perk for running applications.

The Hale system uses the POR mechanism to check information stored in different clouds, and it can verify the repeatability of different copies and check the availability and integrity. The Hale system uses the POR mechanism to check information stored in different clouds, and it can verify the repeatability of different copies and check the availability and integrity. **[1] [25]**

**Image (b): Typical Information Security in Cloud Computing [42]**




## 3. INFORMATION CONFIDENTIALITY

Information privacy is critical for users to keep their personal or confidential information in the cloud. Verification and accessibility techniques used to

ensure the confidentiality of it. Data protection, confirmation, and issue controlling access to distributed computing tended to by expanding cloud unwavering quality and dependability. Because trusted users of cloud providers and cloud storage service providers are unlikely to eliminate the internal threat, it is perilous for users to store their sensitive information in direct cloud storage.

Simple encryption deals with the key management problem and will not support complex requirements such as query, parallel conversion, and good authorization. **[33] [1]**

- **HOMOMORPHIC ENCRYPTION**

Encryption commonly used to ensure information privacy. Homomorphic encryption is a sort of encryption framework. Homomorphic encryption ensures that the results of the ciphertext algebraic operation are consistent with the explicit action following the encryption result; Furthermore, there is no need to decrypt it for the entire process. Implementation of this technology can significantly address the confidentiality of information and information operations in the cloud. Gentry first proposed a fully homomorphic encryption method that allows any action to performed without decrypting in plain text. The ciphertext is a significant breakthrough in homomorphic encryption techniques.

However, encryption systems are very complex, and the costs of computing and storage are very high. Homomorphic encryption maybe even far from accurate applications. A cryptographic algorithm called Diffie-Hellman proposed for secure communication that is very different from critical distribution management systems. For greater convenience and increased security, a hybrid technology that combines multiple encryption algorithms such as RSA, 3DES, and random number generators proposed. RSA can be used to establish secure communication connections through digital signature-based authentication; in contrast, 3DES blocks are useful for information encryption **[35] [2] [9].**

- **ENCRYPTED SEARCH AND INFORMATION BASE**

Homomorphic encryption is a kind of encryption structure. That examines the utilization of limited homomorphic encryption calculations in the cloud condition. Encrypted search is a simple operation. Memory-less data-based encryption innovation has been proposed for the protection and security of touchy data in untrusted cloud situations. There is synchronization between owner and customer to gain access to information. The client needs a key from the synchronizer to decrypt the encrypted shared information received from the owner.

The synchronizer used to store synchronized information and keys separately. The downside of this method is that it tends to be postponed because of extra correspondence with the focal synchronizer. However, this limitation can be reduced by adopting group encryption and reducing communication between nodes and synchronizers.

A multi-keyword rank search procedure that protects privacy over encrypted cloud information is proposed [29]that enables users to search encrypted cloud information and rank search results without leaking privacy. **[14] [8]**

- **HYBRID TECHNIQUE**

A hybrid technique for information privacy and integrity is proposed that uses both key sharing and authentication techniques. Connectivity between user and cloud service providers can be made more secure by using robust key sharing and authentication processes. The RSA public key algorithm can be used for the secure delivery of keys between the user and the cloud service providers. The three-tier information security technology proposes that the first layer for cloud user authenticity be used by one factor or twice; the second layer encrypts the user's information to ensure security and confidentiality, and the third layer rapidly restores it through the decryption process. **[40][15]**The cloud-based event-based isolation of critical information, Trust Draw, combines transparent security extension for the

cloud, virtual machine intersection (VMI), and reliable computing (TC)**[3].**

- **INFORMATION CONCEALMENT**

Concealer can also be used to manage information privacy in the cloud. Information Hides View merges real information with duplicate information. However, authorized users can easily duplicate and separate duplicate information from real information. Information hiding techniques increase the total volume of real information and provide increased security for personal information. The purpose of information hiding is to keep real information safe and secure from malicious users and attackers. The watermarking method is crucial for real information. Watermarking is the key only for users with authorization, so user authentication is essential for accessing the right information to the right users.**[23][18]**

- **DELETION CONFIRMATION**

Deletion Confirmation means that users cannot retrieve information when they have removed their information after confirmation of the deletion. The problem is more severe because there is more than one copy in the cloud to protect and facilitate information recovery. All copies of it must be removed at the same time when users delete their information with the confirmation. However, some information recovery methods can recover data that users have withdrawn from the hard disk. Therefore, Cloud storage providers need to ensure that the removed information of users is not retrieved and that other unauthorized users cannot use it **[39].**

One possible approach is to encrypt it before it is uploaded to the cloud storage space, retrieve it, and avoid unauthorized use. The feed system is based on techniques such as optimizer. On the system, it was encrypted before being uploaded to the cloud storage. When users decide to delete their information, the system is only covered with new information to change the delete operation to implement a strategy specific to all storage spaces **[38][4].**

**Image(c): Costs of Cloud Computing in multiple Organization [43]**


## 4. INFORMATION AVAILABILITY

Data accessibility is as follows: In mishaps, such as hard circle harm, IDC fire, and system disappointments. How much valuable data can be utilized or recovered, and how clients depend on their credit ensure as opposed to strategies, Cloud specialist organizations just confirm the data. The issue of storing information on a Trans border server is a severe concern of consumers, as local laws govern cloud vendors; therefore, cloud clients need to know those laws. Additionally, cloud service providers must ensure information security, especially information privacy and integrity. **[17]**

The cloud providers must share all such concerns with a customer and build a trusting relationship in this regard. The cloud vendor must guarantee information security and explain the jurisdiction of local laws to customers. The paper's crucial point of convergence is on data issues and issues identified with a data stockpiling area and its exchange, costs, accessibility, and security. Information recognition helps users build confidence in the cloud. Cloud storage offers a transparent storage service for users **[29][7].**

- **RELIABILITY OF HARD DRIVE**

Hard drives are currently the primary storage medium for cloud environments. Hard disk reliability is the foundation of cloud storage, hard drive error rates based on hard-drive historical information. They found that hard-drive error rates were not closely related to the temperature and frequency used, whereas hard-drive error rates had strong clustering characteristics.

The most common abnormal behavior of trusted storage is that cloud service providers may leave some of the user's updated information that is difficult to verify based on simple information encryption. Generally, a good storage agreement requires a simultaneous change to support multiple users. However, the types of operations supported by the trusted storage protocol are limited, and most calculations only take place in clients. It can effectively prevent attacks and leave other vulnerabilities in the trusted cloud storage environment (e.g., Amazon S3). It enables secure and reliable real-time interaction and collaboration for most users **[1][32].**

## 5. INFORMATION PRIVACY/PROTECTION

Assurance is the limit of an individual or social occasion to release themselves or information about themselves and show them selectively. In the cloud, privacy means when users visit sensitive information, cloud facilities can prevent an adversary from interfering with user behavior through a user visit model not information management **[2].**

Privacy has the following elements:

- Users would be relieved if their friends requested their information. Clients dislike the warnings sent consequently and consistently.
- Extra the client may permit his data to be accounted for as a legacy district rather than a particular spot.

Other users may compromise user information. Reuse innovation is generally utilized in distributed storage, which implies a similar data we, as a rule, reestablish once, however, imparted to a wide range of clients **[22].**

Cloud storage will reduce storage space and reduce the costs of cloud service providers, but attackers can access it by knowing the hash code of the stored files. After that, it is possible to leak sensitive information into the cloud. So the proof of ownership has been proposed to test the authenticity of cloud users. Attackers can lead to an increase in the costs of cloud service. The use of fraudulent resources is a form of attack on the payment of a cloud service. Attackers can use some information to increase the costs of cloud service payments. **[28][38]**

Cloud computing facilitates a large number of shared resources on the Internet. Cloud systems should be able to avoid Denial of Service (DoS) attacks. A reliable model should have privacy features, trust domains that build capabilities, and robust facilities. Cloud computing requires the user to transfer his information to the clouds based on reliability.**[13]**

Cloud technology has given opportunities to several businesses to showcase their potential within the business world. SMEs don't seem to be solely obtaining a chance to grow, and they're additionally taking their business operations to the following level. Cloud technology has opened a door for small& medium scale firms to accumulate market share by getting into the yard of more significant players. Because the business necessities became on-demand and need-based, it gave several firms a considerable edge and permitted them to complete in a very abundant, more significant business area. Cloud technology offers varied benefits. They are ranging from information management, information storage, 1/3 period, CRM management, resource improvement to entire business automation. It additionally reduces a high quantity of investment and saves a great deal of your time **[8][9].**

- **COMPARISON OF INFORMATION SECURITY IN CLOUD OVERYEARS.[32][1][10][33][28]**

| 2000-2005 | 2005-2010 | 2010-2015 | 2015-2020 |
|---|---|---|---|
| ➢ Utility computing<br>➢ It offers resources and infrastructure management to the customer as per their demand. | ➢ Static and dynamic information handling. Efficiency (Computation, Communication, Storage) | ➢ Cloud platforms were preferred over information centers to increase cloud security. | ➢ Increases storage capacity and enhances the performance of the Internet by maintaining the quality of data. |
| ➢ Introduction of<br>➢ IAAS<br>➢ PAAS<br>➢ SAAS | ➢ Privacy preservation<br>➢ Security<br>➢ Deduplication | ➢ Information coloring and software watermarking were presented for information security and privacy. | ➢ Expanding Capabilities and lower energy costs by maintaining the quality of services. |
| ➢ Clients are charged for them as you go premise with no direct costs. | ➢ Amazon web facilities were launched and provided strong information security. | ➢ IBM announced the IBM SmartCloud framework. | ➢ Service legal agreement (Geolocation) and assuring the deletion of information from the cloud. |

## 6. CONCLUSIONS

Distributed computing is a promising and creating development for next-generation IT applications. Obstacles and barriers to the rapid growth of cloud computing are issues of information security and privacy. Reducing information storage and processing costs is a must for any organization. Still, analysis of information and information is always a critical task in all organizations for decision making. Therefore, no company transfers its information or information to the cloud until trust established between cloud service providers and customers. Researchers have proposed several methods for information protection and the highest level of information security in the cloud. However, there are even many gaps to be made to make these methods more effective. There is much work to be done in cloud computing to make cloud computing acceptable to users. This paper surveyed multiple techniques about information security and privacy to build trust between cloud computing providers and customers for information security in cloud computing environments. **[18][17]**

Cloud computing techniques can provide banks with a competitive advantage in the market, costs reductions, higher margins, simplified maintenance and management of applications across the enterprise, greatly extended scalability, agility, high availability, automation, large information storages, and reliable backup mechanisms. Banks may explore

the use of cloud computing initially for better performance through peak demand.

Though the current adoption of cloud computing at banks is low, the benefits it assures will result in cloud computing gaining prominence and the years. This advancement is because cloud computing has helped several enterprises **[6].**

## 7. CONFLICT OF INTERESTS

We declare that there is no conflict of interest regarding the publication of this paper. Also, all the provided information in this paper is accurate under my knowledge.

## 8. REFERENCES

1. N. Leavitt, "Is cloud computing prepared for key cadence?" Personal computer,vol.42,no.1,pp.15–25,2009.
2. D. Chen and H. Zhao, "Information security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE'12), vol.1,pp.647–651, Hangzhou, China, March 2012.
3. D.Feng et al. "Study on cloud computing security." Journal of Software 22.1 (2011): pp.71-83.
4. Deyan, C., & Hong, Z. (2012, 23-25 March 2012). Information Security and Privacy Protection Issues in Cloud Computing. Paper presented at the Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on.
5. Mell Peter and Grance Tim, "Effectively and securely using the cloud computing paradigm" [online] 2011,http://csrc.nist.gov/groups/SNS/cloud computing/cloudcomputing-v26.ppt (Accessed 18 August 2013).
6. Cloud Computing Definition. 2011; Available fromhttps://www.nist.gov/newsevents/news/2011/10/final-version-nist-cloudcomputing-definition-published
7. Reagan, P., and Y. Pawar. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Information Security.
8. Chennai, KK, L. Muddana, and RK Tuvalu. Performance analysis of multiple encryption algorithms for usage in multistage encryption for securing information in the cloud. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017
9. Deepali, and K. Bhushan. DDoS attack defense framework for the cloud using fog computing. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017.
10. Sharma, P.K., et al. Issues and problems of information security in a cloud computing environment. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics, and Mobile Communication Conference (UEMCON). 2017.
11. Problems Faced by Cloud Computing, Lord CrusAd3r,dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf
12. Joshua Kissoon, Cloud Computing Security Issues and Solutions, 2013 Counties, and A. G. Bakirtzis, "Bidding strategies for electricity producers in a competitive electricity marketplace," IEEE Trans. Power System, vol. 19, no. 1, pp. 356–365, Feb. 2004
13. K. Hwang and D. Li, "Trusted cloud computing with secure resources and information coloring,"IEEEInternetComputing,vol.14,no.5, pp.14-22,2010.
14. A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing information leakage from indexing in the cloud," in Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD'10),pp.188–195, July 2010.
15. R. Ranch, B. Bhargava, L. B. Othmane et al., "Protection of identity information in cloud-computing without a trusted third party," in Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems(SRDS'10),pp.368–372, November 2010

16. R. Yeluri, E. Castro-Leon, R. R. Harmon, and J. Greene, “Building trust and compliance in the cloud for facilities," in Proceedings of the Annual SRII Global Conference(SRII'12), pp. 379–390, SanJose, Calif, USA, July 2012.
17. J. Idziorek, M. Tannian, and D. Jacobson, “Attribution of Fraudulent Resource Consumption in the cloud,” in Proceedings of the IEEE 5th International Conference on Cloud Computing (CLOUD'12),pp.99–106, June 2012
18. E.Stefanov,M.vanDijk,E.Shietal.,“Pathoram: a straightforward oblivious ram protocol," in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp.299–310, ACM,2013.
19. Delettre, C., Boudaoud, K., &Riveill, M. (2011, 28 June 2011-July 1 2011). Cloud computing, security, and information concealment. Paper presented at the Computers and Communications (ISCC), 2011 IEEE Symposium on.
20. Anane, R., Dhillon, S., &Bordbar, B. (2008). Stateless information concealment for distributed systems. Journal of Computer and System Sciences, 74(2), 243-254.
21. Delettre, C., Boudaoud, K., &Riveill, M. (2011, 28 June 2011-July 1 2011). Cloud computing, security, and information concealment. Paper presented at the Computers and Communications (ISCC), 2011 IEEE Symposium on.
22. They were ensuring information storage security in Cloud Computing. Paper presented at the Quality of Service, 2009. IWQoS. 17th International Workshop on.
23. Cong, W., Qian, W., Kui, R., &Wenjing, L. (2009, 13-15 July 2009). Ensuring information storage security in Cloud Computing. Paper presented at the Quality of Service, 2009. IWQoS. 17th International Workshop on. [
24. ] Leistikow, R., &Tavangarian, D. (2013, 25-28 March 2013). Secure Picture Information Partitioning for Cloud Computing Facilities. Paper presented at the Advanced Information Networking
25. ] Reagan, P., &Pawar, Y. (2013, 6-8 April 2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Information Security in Cloud Computing. Paper presented at the Communication Systems and Network Techniques CSNT), 2013 International Conference on.
26. ] Taeho, J., Xiang-Yang, L., Zhiguo, W., &Meng, W. (2013, 14-19 April 2013). Privacy-preserving cloud information access with multi-authorities. Paper presented at the INFOCOM, 2013 Proceedings IEEE.
27. Gawali, M. B., &Wagh, R. B. (2012, 6-8 Dec. 2012). Enhancement for information security in the cloud computing environment. Engineering (NUiCONE), 2012 Nirma University International Conference on.
28. It was implementing a digital signature with an RSA encryption algorithm to enhance its security of cloud in Cloud Computing. Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.
29. Bashing, S., &Kavitha, V. (2011). A study on security issues in administration conveyance models of distributed computing. Diary of Network and Computer Applications, 34(1), 1- 11.
30. NIST SP 800-145, “A NIST definition of cloud computing”, [online]2012, http://csrc.nist.gov/publications/drafts/800 145/Draft-SP- 800-145_cloud-definition.pdf (Accessed:23 December 2013).
31. Negotiating the cloud – legal issues in cloud computing agreements Commonwealth of Australia 2012, ISBN 978-1-922096-05-0
32. Chennai, KK, L. Muddana, and RK Tuvalu. Performance analysis of multiple encryption algorithms for usage in multistage encryption for securing information in the cloud. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017.
33. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud information, "IEEE Transactions on Parallel and

Distributed Systems, vol. 25,no.1,pp.222–233,2014.
34. S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Government Information Quarterly, vol. 27, no. 3, pp. 245–253,2010
35. R. Yeluri, E. Castro-Leon, R. R. Harmon, and J. Greene, "Building trust and compliance in the cloud for facilities," in Proceedings of the Annual SR II Global Conference.
36. C. Gentry, A fully homomorphic encryption scheme [Ph.D.Thesis],StanfordUniversity,2009.
37. R. Chow, et al."Controlling information in the cloud: outsourcing computation without outsourcing control," presented at the Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009.
38. Image(a):www.grantthornton.com/library/articles/advisory/2018/cyber-risk-information-protection-privacy. aspx
39. Image(b):https://www.uscybersecurity.net/csmag/information-security-privacy/
40. Image(c):https://www.forbes.com/sites/louiscolumbus/2014/12/26/kpmgs-2014-cloud-computing-survey-enterprises-quickly-moving-beyond-costs-reduction-to-customer-driven-results/