Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

26

Cloud Privacy and Security- A Review Paper

Rajan Jha

School Of Computer Science AndApplication

Mit WPU, Pune

1132210594@mitwpu.edu.in

Nikita Kumari

School Of Computer Science AndApplication

Mit WPU, Pune

1132210590@mitwpu.edu.in

Chidera Carol Omeribe

School Of Computer Science AndApplication

Mit WPU, Pune

1132210760@mitwpu.edu.in

Abstract

Distributed computing has revolutionized the way people use cloud resources to host and deliver various services through the internet. The benefits of cloud resources are many, and with the rapid development of cloud technology, it has become more accessible to users. However, one major issue that needs attention is cloud security. Many users are still unaware of the risks associated with cloud storage, and there is a lack of mass awareness on this issue. As cloud technology continues to gain traction in the corporate world, clients need to be aware of the standards of cloud utilization. However, many clients may lack knowledge about IT security, which can be a major risk. It is crucial to measure the level of their understanding

and develop a training framework to promote security awareness. This is where new measurements and calculations for assessing security familiarity come in. By incorporating emerging cloud security requirements, we can better equip corporate clients and workers with the necessary knowledge to use cloud resources safely and securely.

Index Terms- Review, data security, cloud data hiding, security in the cloud

I. INTRODUCTION

The emergence of distributed computing has become a significant area of interest for both academics and business. It presents users with access to web-based services, allowing them to use different software without installing or coopting them based on their prejudice. NIST, the National Institute of Standards and Technology, claims, On-demand network access to a participating pool of adjustable computing offers is provided by distributed computing. However, implementing a successful cloud strategy can be challenging, with data security being a top priority for clients. A 2011 survey conducted by the IDC revealed that clients are concerned about their confidential information being differently applied or moved to a different cloud four types of data that need to be protected include usage data, sensitive financial records, personally identifiable information, and unique device characteristics. Risks associated with distributed computing have been categorized into legal, strategic, operational, and technical risks, with data security identified as the most significant.

Affinity for Cloud Security has highlighted the risks associated with distributed computing fall into thirteen main categories., with data protection being directly or indirectly linked to five of the seven most significant threats. To enhance security, organizations and departments worldwide have conducted research on cloud security advancement, taking into account six perspectives, including data privacy, trust, access control, resource access control, recovery, and separation. Ensuring security at every stage of the data life cycle, including creation, transfer, use, sharing, storage, and destruction, is essential for building clients' trust in distributed computing. Although the goal of distributed computing is to provide better satisfaction and reduce clients' responsibility, security risks still exist and need to be addressed.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

II. ORDER OF CLOUD REGISTERING

Distributed computing is an increasingly popular method of accessing services over the internet without having to purchase or install software on personal computers. Its advantages include multi-tenure, high scalability, flexible payment options, and asset self-provisioning. The administrative Three categories are included in the cloud computing model: IaaS, PaaS, and SaaS. IaaS provides Internet-based, virtual computing environment computing resources and systems administration elements, while PaaS enables developers to create applications in various programming languages. SaaS allows clients to use internet resources hosted by service providers, such as software and apps. Cloud computing modes of deployment that are public, private, hybrid, and community clouds. However, public clouds deployment presents a significant risk to information security.

While clients rely on service providers for security measures, they are also at risk of data breaches. It is essential for service providers to put in place stringent security procedures to safeguard client data and gain their trust. Previous reviews of security issues with cloud computing have been limited and lacked detailed analysis. In this study, we conducted a thorough literature review to focus about the public cloud's concern with data security deployment for distributed enumerate

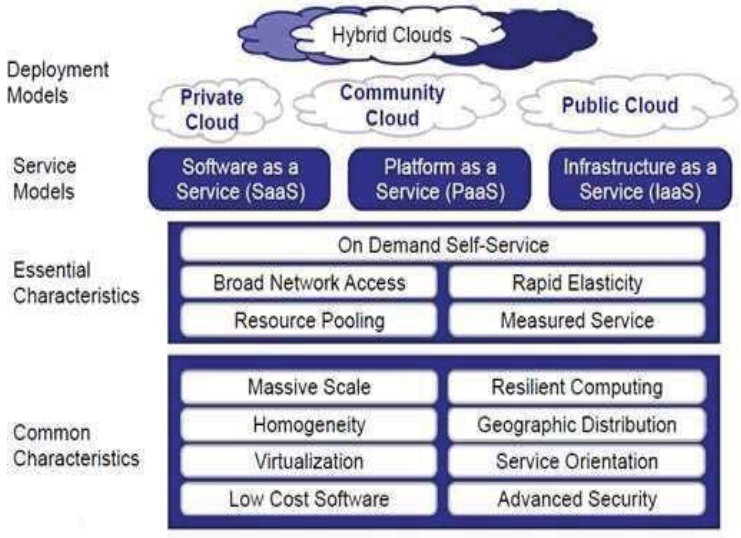


Figure 1 Cloud Foundation for NIST

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

III. METHODOLOGY

When researching computers, researchers are increasingly conducting systematic literature reviews to examine a broad range of topics. This research work builds upon a literature review presented in reference 24, and Figure 3 depicts the review procedure. An organised literature review aims to deliver an extensive overview of recent writings pertinent to a specific question. Numerous scientists have adopted these principles to contribute to the field of software engineering. For example, previous studies such as references 25 and 26 have used a systematic literature review process to evaluate aspects evaluation of software product line components and software component reuse methods. The literature Three phases and 10 sub-activities make up the review process. During the first phase, researchers introduce a set of questions to guide the review.

Que. 1 What methods are known for ensuring data security in cloud assessment?

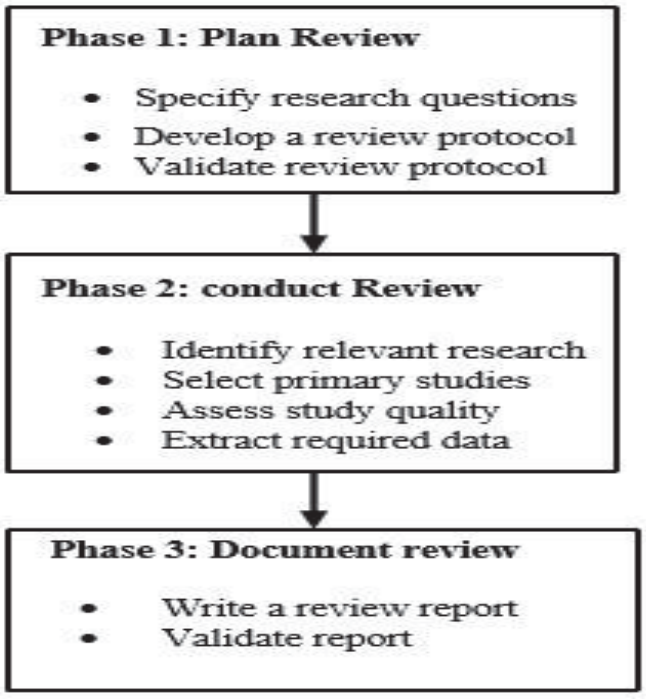


Fig. 2: Review procedure modified from [24].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Que 2. How have the procedures been authorized?

The first sub-activity of Stage 1 in this research study involved developing a survey protocol that included the sources and keywords to be used. The protocol was reviewed, analyzed, and modified by researchers before the final version was presented in Table 1. The sources used for this study included ScienceDirect, IEEE Xplore, Google Scholar, Scopus, ACM Digital Library, and JSTOR. The study focused on research papers published between 2007 and 2021.

Table 1. Review protocol

Year	sources	Key words
2007-2014	IEEE Xplore, science direct, Scopus, Google scholar, ACM portal digital library, IJERA, IJSI	Cloud computing, cloud computing security, data security/data concealment, cloud data security, cloud data storage

In the second period of the audit, the hunt is performed by involving various questions connected with information security in cloud processing climate. The underlying During the second stage of the review process, a quest was carried out utilizing lively queries on data security in cloud computing. The studies were evaluated based on certain quality criteria, including the presence of a model, experiment, system, or guideline. Relevant data based on the documents was collected to respond to the research inquiries. To ensure that no critical references were missed, an additional step was taken to search the references of the selected papers. The information gathered was combined to present the overall results. The evaluation process's last stage involves thethe findings were analyzed and a comprehensive report was written and approved. The systematic literature review process followed in this study was based on established principles and protocols used in previous research studies, such as those presented in [25, 26].

IV. RESULTS

In this section, we will be presenting the results obtained from the survey. As a way to offer a thorough and detailed an overview of the results, table 2 has been included, which displays a yearly summary of the number of papers published citing sources. To complement this,

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Figure 4 has also been included to visually represent the outcomes. These findings will be presented in detail in relation to the research questions that were previously stated.

Table 2 year wise search results

Year	No. of papers
2007	0
2008	1
2009	1
2010	5
2011	5
2012	8
2013	9
2014	2
2015	5
2016	3
2017	8
2018	5
2019	1
2020	3
2021	3
Total	59

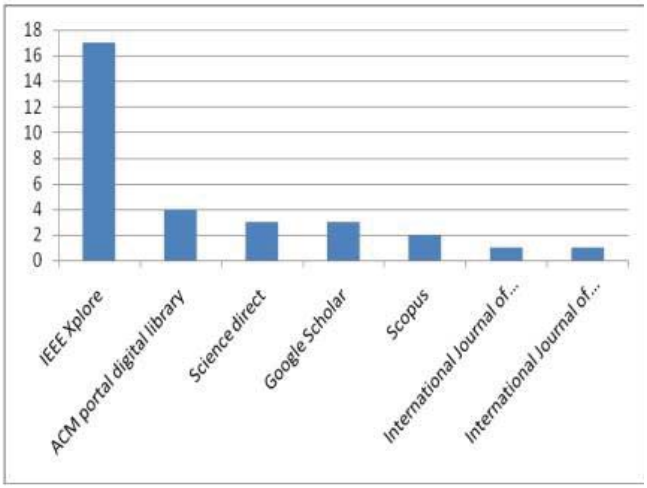


Fig4: Frequency of papers w.r.t to sources

Que. 1 What methods are known for ensuring data security in cloud assessment?

The audit findings resulted in the proposal of recommended methods for the distributed evaluation of intelligence security, as illustrated in Figure 5. The figure groups the results into decoding, where the scheme text denotes the year and the number of published papers. The survey process involved three stages, each with ten sub-activities. During the first stage, the review was planned, research questions were specified, a survey convention was developed, and the audit convention was validated. In the second stage, the review was conducted, relevant studies were identified, primary studies were selected, the quality of the studies was assessed, required data was extracted, and information was synthesized. In the third stage, the review was documented, and the report was validated. these findings, which were transformed into figure text using various encryption algorithms.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Table 3 category wise results of question1

Question	category	No. of papers
What approaches have been introduced to ensure data security in cloud computing?	Encryption	14
	Homomorphic token	2
	Sobol sequence	1
	Guideline	6
	Harmonizing scheme	1
	Data concealment component	1
	Framework	5
	Stripping algorithm	1
	Total	31

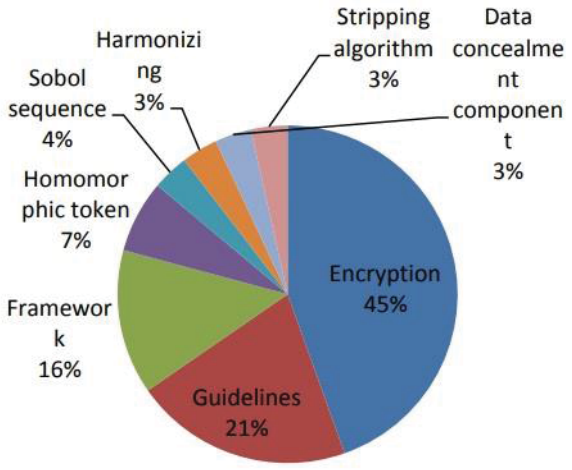


Fig 5: Proposed approaches to ensure data security

V. AUTHENTICATION

A The results of the show that encryption (45%) was the most widely employed technique to ensure cloud computing data security. In order to secure a computerized signature algorithm using RSA encryption is proposed in [27]. This algorithm employs a "hashing computation" technique in programming to reduce a big number of lines of data into a smaller number of lines. The message digest is then encoded using the sender's digital signature using a private key. The sender's private key and the recipient's public key are used by the programme to decode the digital signature into a message digest. In [28], SDES (Simplified Data Encryption Standard) and Data Encryption Standard (DES) core elements are coupled with the Vigenère and Playfair cypher techniques. The "black box" is used to divide plain text into equal portions, with 2 pieces on the right and 6 pieces on the left. These 6 pieces are further separated into two parts, with the first two pieces representing the columns and the last four pieces representing the rows. Finding the rows and columns will yield the relevant value. The resulting 64-bit block is then subjected to the predominant function block, which has a fixed block size of 64 cycles. Each of the 8 octets of the resulting Vigenère block, composed of 64 bits, is then subjected to this function.

Finally, these components are further separated into smaller blocks. According to the research, encryption was the strategy most frequently employed to assure the security of cloud data, accounting for 45% of the cases studied. One proposal presented in [27] employed an RSA-encrypted digital signature algorithm for securing cloud data. The approach utilized a "hashing computation" technique to reduce large data collections to a manageable amount of lines. This message digest was then encoded with the programmer's confidential key to generate a digital signature. In [28], a method was proposed that combined Data Encryption Standard (DES) core pieces with the Playfair and Vigenere cipher, and cipher techniques. Another approach utilized Bilinear Diffie-Hellman in [29] for secure key exchange, with RSA employed for data encryption. It's allowing for secure communication between clients and clouds without external servers. Prior to transmission to the cloud, the client added a heading to the message information and encrypted the data. [30] used Data security is ensured by Secure Socket Layer (SSL) 128-bit encryption. availability, integrity, confidentiality, which could be increased to 256-bit encryption.

In [31], the client delivered the cloud-based data, and the supplier of clouds generated a keychain, encrypted client data using the I saved the RSA algorithm.it on it's server farm. [32] proposed a three-layered information security model, with each layer responsible for securing the data in the cloud. Finally, [33] utilized the RC5 algorithm to retrieve information from the cloud, with scrambled data conveyed to ensure that it could not be decoded even if intercepted. In order to guarantee the safety of data in the cloud, various methods have been proposed. Encryption has been found to be the most commonly used method, with different techniques such as RSA-encrypted digital signature algorithm, DES basic components with the Playfair and Vigenere encryption, Simplified Data Encryption Standard (SDES), and techniques, Bilinear Diffie-Hellman, and RSA being utilized.

Other methods that use access control mechanisms to ensure data security include (RBE) and Role Base Access Control. Safe distributed computing has been proposed secret sharing utilising symmetric bivariate polynomial-based cryptography and elliptic Diffie-Hellman (ECDH). Area-based encryption has also been suggested using client area and topographical position, while a combination of computerized Advanced Encryption with Diffie Hellman key exchange and signature Standard encryption computation It been suggested that secure

cloud-based categorization of data. Another approach is three layered information security model that has introduced to cloud-based protected data.

VI. INSTRUCTION

The safety of data stored in the cloud canensured through various approaches, as revealed by our survey. One such approach is the use of rules, as demonstrated in [21], where rules were employed to ensure data security. [39] presented a new cloud framework engineering method that involved three key features, including the partition and system service providers, the withholding of information regarding the owners of the data, and the obscuring of the data. Another approach is the use of specialists, as described in [40], where a specialist policy was developed to protect data in cloud architecture, utilizing three specialists, include experts in files, authentication, and keys management specialist.

[41] provided rules for six key information technologies, including data security protection, verification of the both exist and availability of data, reliable access management, and trusted cloud resource access control. Finally, [42] presented rules for selecting the best encryption algorithms based on an evaluation of four distinct encryption techniques, which can be helpful in choosing the most suitable algorithm according to the needs of the user.

VII. SUBSTRUCTURE

To enhance data security in the cloud, several system approaches have been suggested. One such approach is the trusted cloud system that utilises data-driven criminal investigator method for increasing data safety. a system incorporates file-driven and information-driven logging tools to enhance data privacy. Another approach is the multi-tenant framework that comprises three layers, including presentation, High security for user data is provided by business logic and data access layers. A protocol called "sec cloud" has been proposed that combines Using a specified verifier signature, group authentication, and probabilistic encryption, safe data storage and computing in a cloud environment testing methods. In addition, a three-phase approach has been suggested that involves data categorization and metadata indexing Multi-user private encryption with keyword access is used to provide total data privacy. to keep resulting records secret from cloud service providers, and a policy to aid

data sharing among users using metadata and encryption schemes. These system approaches help make sure that data on the cloud is secure and private.

VIII. RESEMBLANCE TOKEN

An innovative method has been suggested to dependable and effective dynamic operations the data blocks the cloud. method involves use of resemblance tokens with spread verification of erasure-coded data, which allows for secure data deletion, update, and attachment. The proposed approach builds upon a similar model proposed in [48] and employs a token precalculation technique to achieve storage RI integration. By implementing the resemblance token scheme, this approach addresses seven critical issues identified in [47]. The unique features of this method make it a promising approach for enhancing data security and privacy in the cloud.

IX. STRIPING CALCULATION, INFORMATION COVERING PART, ORCHESTRATING, AND TOKEN PLOT.

To ensure secure retrieval of calculation data images in the cloud, a combination of fragmentation and token schemes have been proposed. This approach addresses three critical issues highlighted in [49]: data dissemination, data fragmentation, and image analysis. Another data partitioning scheme was proposed in [50], consisting of Data production, data tagging, and prediction are the three sub-parts. the evaluation of this scheme demonstrated its effectiveness in protecting genuine user data and defending against potential attacks.

In [51], a security-preserving repository was established with a primary focus on achieving information privacy while maintaining seamless relations within a cloud. This suggestion approach enables owners delegate especially the chores that need a lot of computes to cloud servers without revealing the elements of the data. Similarly, in [52], a scalable and efficient verification protocol was proposed to discuss about computing data security. Instead of using pseudorandom data, this approach combines token precomputation using Sobol sequences to verify the integrity of erasure-enciphered data. The suggested design consists in three phases: document distribution, token precomputation, as well as the challenge-response procedure.

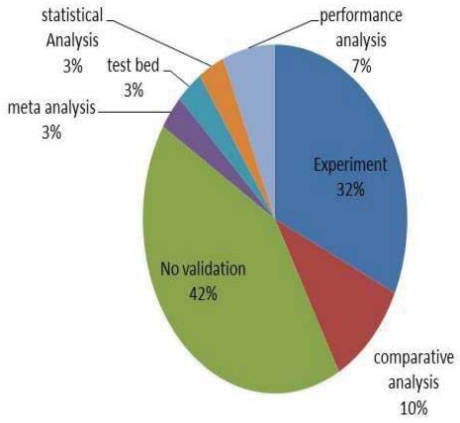
Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Que 2. How have the procedures been authorized?

Figure 6 presents the second investigation's findings. which displays various methods utilized for validating the proposed approaches. The classes include: (1) experimentation, which involves conducting trials (2) Comparative analysis to verify the results, which involves comparing the suggested approach with other methods to validate the results; (3) testbed, which involves validating the proposed approach on a testbed; (4) statistical analysis, which involves analyzing the results using some statistical method; (5) meta-analysis, which involves validating the results through a systematic review of existing literature; (6) performance analysis, which involves analyzing the performance of the proposed approach using different methods; and (7) presented strategies that lack any form of validation. Table IV provides the order confirmation information. and Figure 6 illustrates the percentage of each validation type. Any exact procedure is referred to as validation utilized evidence, excluding the mere utilization of the proposed approach.

Table 4 categories wise results of question 2

Question	category	No. of papers
How the approaches have been validated?	Experiment	10
	No Validation	13
	Comparative Analysis	3
	Meta Analysis	1
	Test Bed	1
	Statistical Analysis	1
	Performance Analysis	2
	Total	31



The investigation into whether proposed methods were validated revealed that although 47% of the cited studies suggested a method for protecting data in pall terrain, they failed to provide any supporting evidence.

X. CONDUCTING TESTS

Several papers from the selected ones have proposed different approaches and conducted experiments to validate their proposed models. In one study [32], the proposed model was tested using a cloud test system named Hadoop, which involved implementing three security measures: message authentication code, data file arrangement, and encryption. Another study [33] used programme in the pall landscape to verify the outcomes of the rc5 algorithm, and the outcomes were contrasted with those of the Amazon S3 service. Microsoft Net Fabrics-based linked networks may be built and run using Aneka. In a different study [34], the proposed design was implemented in Java, and the outcomes shown that the efficacy of encryption and decryption is very good and that the size of the plaintext is precisely proportional to the size of the ciphertext. The findings also revealed that the decryption key's size is 48 bytes, which is advantageous for drug users.

In yet another study [39], a cloud service was approach using C# Microsoft .net frame for attestation group cooperation. According to the trial's results, the service response time increases linearly as input textbook size is increased and data de-obfuscation does not result in significant outflow. The performance test also revealed the impact of partitioning on data production. The suggested technique encompassed data generation, data trailing, and data birth. Overall, these studies have proposed various approaches and conducted experiments to validate their proposed models, which can be helpful in securing data in the cloud environment.

XI. RELATIVE ANALYSIS

To support the suggested approaches, 10 % of the chosen studies used comparative analysis as a type of validation, in which the outcomes of the proposed approach are compared with those of other approaches. In [53], a comparison study was carried out to confirm the findings by taking into account elements like granularity, key management, and meta-information Administration, level of verification, and secret sharing. The proposed method utilized both trusted and an unreliable third parties. [28] outlines the suggested encryption method was validated by comparing it with input from both Playfair and Vigenere. This comparison helped to validate the proposed approach's results and ensure that they were accurate and

reliable.

XII. ANALYTICAL ANALYSIS

A small percentage of the selected papers (3%) use empirical testing, meta-analysis, and proof of concept as validation methods. For instance, in [32] and [42,52], empirical tests from NIST are employed to verify the findings by selecting eight modern encryption schemes. A meta-analysis of four distinct security algorithms was conducted in another research, including RSA, Blowfish, together with DES, is shown in terms stage utilization flexibility, limit verification type, memory requirements, and time of operation. Moreover, to support the outcomes, a proof of concept is developed and tested.

XIII. ENDS AND FUTURE BEARING

Distributed computing has numerous benefits, such as costeffectiveness, fast data transmission, and improved accessibility. However, several critical issues need to be addressed, particularly with regards to data security. Numerous researchers have made contributions to developing various solutions, which are reviewed in this paper. A literature review of cloud computing data security is carried out, and the outcomes reveal that most approaches rely on encryption. Out of 45 encryption methods reviewed, 71% of the results were validated through some form of validation, with 67% of encryption strategies using trial and error to validate the outcomes. These findings suggest that most researchers are interested in the encryption process to improve data security in the distributed computing environment.

REFERENCE

[1] 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).

[2] Gartner, "What you need to know about cloud computing security and compliance" (Heiser J), [online] 2009, https://www.gartner.com/doc/1071415/-need-knowcloud-computing- Security (Accessed 23 December 2013).

[3] IDG Cloud Computing Survey: "Security, Integration Challenge Growth", [online]http://www.forbes.com/sites/louiscolumbus/2013/08 /13/idg- cloud-computing-

survey- (Accessed: 28 December 2013).

[4] Ricadela, "Cloud security is looking overcast" [online] http://www.businessweek.com/magazine/cloudsecurity-is-lookin g-overcast-09012011.html. (Accessd: 29December 2013).

[5] Nguyen, "Only seven percent of UK its services in the cloud, says survey, Computerworld" [online] http://www.itworld.com/ cloudcomputing/200657/only-seven-percent-uk-itservices-cloud-says- surveyS. (Accessed: 29 December 2013).

[6] Elahi, T., & Pearson, S. (2007). Privacy Assurance: Bridging the Gap Between Preference and Practice. In C. Lambrinoudakis, G. Pernul & A. Tjoa (Eds.), Trust, Privacy and Security in Digital Business (Vol. 4657, pp. 65-74): Springer Berlin Heidelberg.

[7] Siani Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," CLOUD'09, May 23, 2009, Vancouver, Canada, pp. 44-52.

[8] European Network and Information Security Agency (ENISA) "Benefits, risks and recommendations for information security" [online] http://www.enisa.europa.eu/-activities/riskmanagement/files/deliverables/cloud-computing-riskassessment.- (Accessed: 28. December 2013).

[9] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing" [online]https://cloudsecurityalliance.org/csaguide.pdf (Accessed 26 December2013)

[10] J. Archer et al., "Top Threats to Cloud Computing," in Cloud Security Alliance [online] https://cloudsecurityalliance.org/topthreats/csathreat s.v1.0.pdf (Accessed: 26 December 2013).

[11] Crampton, J., Martin, K., & Wild, P. (2006, 0-0 0). On key assignment for hierarchical access control. Paper presented at the Computer Security Foundations Workshop, 2006. 19th IEEE.

[12] D.Feng, et al. "Study on cloud computing security." Journal of Software 22.1 (2011): pp.71-83.

[13] R. Chow, et al., "Controlling data 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.

[14] S. Dawn Xiaoding, et al., "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on, 2000, pp. 44-55.

[15] Michael Annbrust etc., Above the Clouds: A Berkeley View of Cloud Computing, http: //eecs.berkeley.edu/Pubs/TechRpts/2009 /EECS 2009-28.pdf:2009.2.

[16] Deyan, C., & Hong, Z. (2012, 23-25 March 2012). Data Security and Privacy Protection Issues in Cloud Computing. Paper presented at the Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on.

[17] Seccombe, A., Hutton, A., Meisel, A., Windel, A., Mohammed, A., & Licciardi, A. (2009). Security guidance for critical areas of focus in cloud computing, v2. 1. Cloud Security Alliance.

[18] T. Mather and S. Latif, "Cloud Security and Privacy, [online] 2009, http://www.slideshare.net/USFstudent1980/cloud- computing security-concerns (Accessed: 4 September 2013)

[19] IBM, "what is cloud computing" [online] http://www.ibm.com/cloud-computing/in/en/what- is-cloud-computing.html (Accessed: 14 December 2013)

[20] Mell Peter and Grance Tim, "Effectively and securely using the cloud computing paradigm" [online] 2011, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt (Accessed 18 August 2013).

[21] 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.

[22] Sarwar, A., & Khan, M. N. (2013). A Review of Trust Aspects in Cloud Computing Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2(2), 116-122.

[23] Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. Procedia Engineering, 15(0), 2852-2856.

[24] Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, 80(4), 571-583.

[25] Fazal-e-Amin, A. K. M., & Oxley, A. (2010). A review on aspect-oriented implementation of software product lines components. Information Technology Journal, 9(6), 1262-1269.

[26] Fazal-e-Amin, A. K. M., & Oxley, A. (2011). A Review of Software Component Reusability Assessment Approaches. Research Journal of Information Technology, 3(1), 1-11.

[27] Somani, U., Lakhani, K., & Mundra, M. (2010, 2830 Oct. 2010). Implementing digital signature with RSA ncryption algorithm to enhance the Data Security of cloud in Cloud Computing. Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.

[28] Vamsee k and sriram r, (2011) "Data Security in Cloud Computing,"in Journal of Computer and Mathematical Sciences Vol. 2, pp.1-169.

[29] Shuai, H., & Jianchuan, X. (2011, 15-17 Sept. 2011). Ensuring data storage security through a novel third-party auditor scheme in cloud computing. Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on.

[30] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 18311838.

[31] Parsi Kalpana & Sudha Singaraju (2012). Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology (IJRCCT), vol 1, Issue 4.

[32] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14-16 May 2012). Enhanced

data security model for cloud computing. Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on.

[33] Singh, J., Kumar, B., & Khatri, A. (2012, 6-8 Dec. 2012). Improving stored data security in Cloud using Rc5 algorithm. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.

[34] Lan, Z., Varadharajan, V., & Hitchens, M. (2013). Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. Information Forensics and Security, IEEE Transactions on, 8(12), 1947-1960.

[35] Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013, 14-19 April 2013). Privacy preserving cloud data access with multi-authorities. Paper presented at the INFOCOM, 2013 Proceedings IEEE.

[36] Ching-Nung, Y., & Jia-Bin, L. (2013, 2-5 July 2013). Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing. Paper presented at the Biometrics and Security Technologies (ISBAST), 2013 International Symposium on.

[37] Abolghasemi, M. S., Sefidab, M. M., & Atani, R. E. (2013, 22-25 Aug. 2013). Using location-based encryption to improve the security of data access in cloud computing. Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on.

[38] Rewagad, P., & Pawar, Y. (2013, 6-8 April 2013). Use of digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. Paper presented at the Communication Systems and Network Technologies CSNT), 2013 International Conference on.

[39] Yau, S. S., & An, H. G. (2010). Protection of users' data confidentiality in cloud computing. Paper presented at the Proceedings of the Second AsiaPacific Symposium on Internetware.

[40] Feng-qing, Z., & Dian-Yuan, H. (2012, 24-26 Aug. 2012). Applying agents to the data security in cloud computing. Paper presented at the Computer Science and Information Processing (CSIP), 2012 International Conference on.

[41] Zhongbin, T., Xiaoling, W., Li, J., Xin, Z., & Wenhui, M. (2012, 27-30 May 2012). Study on Data Security of Cloud Computing. Paper presented at the Engineering and Technology (S-CET), 2012 Spring Congress on.

[42] Rachna, A., and Anshu, P. (Jul-Aug 2013). Secure User Data in Cloud Computing Using Encryption Algorithms in International Journal of Engineering Research and Applications (IJERA), 3(4),19221926.

[43] Ko, R. K. L., Kirchberg, M., & Bu Sung, L. (2011, 3-5 Aug. 2011). From system-centric to data-centric logging Accountability, trust & security in cloud computing. Paper presented at the Defense Science Research Conference and Expo (DSR), 2011.

[44] Gawali, M. B., & Wagh, R. B. (2012, 6-8 Dec. 2012). Enhancement for data security in cloud computing environment. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.

[45] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., et al. (2014). Security and privacy for storage and computation in cloud computing. Information Sciences, 258(0), 371-386.

[46] Rashid, F., Miri, A., & Woungang, I. (2013, June 28 2013-July 3 2013). Secure Enterprise Data Deduplication in the Cloud. Paper presented at the Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on.

[47] Cong, W., Qian, W., Kui, R., & Wenjing, L. (2009, 13-15 July 2009). Ensuring data storage security in Cloud Computing. Paper presented at the Quality of Service, 2009. IWQoS. 17th International Workshop on.

[48] Tribhuwan, M. R., Bhuyar, V. A., & Pirzade, S. (2010, 16-17 Oct. 2010). Ensuring Data Storage Security in Cloud Computing through Two-Way Handshake Based on Token Management. Paper presented at the Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on.

[49] Leistikow, R., & Tavangarian, D. (2013, 25-28 March 2013). Secure Picture Data Partitioning for Cloud Computing Services. Paper presented at the Advanced Information Networking and IJCATM: www.ijcaonline.org Applications Workshops

(WAINA), 2013 27the International Conference on.

[50] Delettre, C., Boudaoud, K., & Riveill, M. (2011, June 28 2011-July 1 2011). Cloud computing, security and data concealment. Paper presented at the Computers and Communications (ISCC), 2011 IEEE Symposium on.

[51] Mishra, R., Dash, S. K., Mishra, D. P., & Tripathy, A. (2011, 8-10 April 2011). A privacy preserving repository for securing data across the cloud. Paper presented at the Electronics Computer Technology (ICECT), 2011 3rd International Conference on.

[52] Syam Kumar, P., Subramanian, R., & Thamizh Selvam, D. (2010, 28-30 Oct. 2010). Ensuring data storage security in cloud computing using Sobol Sequence. Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.

[53] Anane, R., Dhillon, S., & Bordbar, B. (2008). Stateless data concealment for distributed systems. Journal of Computer and System Sciences, 74(2), 243-254.

[54] Bhat, M.I., Sharada, B., Sinha, M.K. (2022). A Graph-Based Holistic Recognition of Handwritten Devanagari Words: An Approach Based on Spectral Graph Embedding. In: Santosh, K., Hegadi, R., Pal, U. (eds) Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2021. Communications in Computer and Information Science, vol 1576. Springer, Cham. https://doi.org/10.1007/978-3-031-07005-1_25