Cloud Privacy and Security-A Review Paper

Saurabh Kumar[1], Shreya Gupta[2], Ayush Vir Singh[3]

Galgotias University

ABSTRACT

Distributed computing hosts and conveys various administrations through internet there are a great deal of reasons why individuals settle on utilizing cloud assets cloud improvement is expanding quick while a great deal of related administrations drop behind for instance the mass attention to cloud security anyway the new age transfer recordings and pictures without motivation to a distributed storage yet just barely any have some familiarity with information security information the board and the restrictive of put away information in the cloud in a venture climate the clients need to know the standard of cloud utilization but they have little information about customary it security it is crucial to measure the depth of their understanding and progress the preparation framework to foster the security mindfulness the article demonstrates the significance of proposing new measurements and calculations for estimating security familiarity with corporate clients and workers to incorporate the prerequisites of arising cloud security.

1.3 1 . INTRODUCTION

Circulated registering a new development that has prompted fundamental consideration in both industry and the insightful world it offers sorts of help over the web by using dispersed figuring clients can utilize the electronic organizations of various programming rather than purchasing or presenting them on their laptops as demonstrated by the public foundation of standard and creativity NIST classification According to Gartner [2], registration is a perspective for utilising supported introduction to a standard pool of movable handling resources on demand. Spread out processing can include portrayed as an approach to calculating that passed it limits as assistance on to end clients through the web. As demonstrated by late concentrate by worldwide information bunch big adventure the three hardships to executing a successful cloud technique in enormous business change basically among It and its finally gotten [3] Information security is a major consideration for customers that need to employ distributed computing, according to a poll conducted by the information association IDC in 2011. The majority of clients of cloud companies have expressed worries about their private information being utilised for other reasons or transferred to another cloud.
professional associations [6] Financial records, among other things, are one of the four categories of client data that must be secured. Information that becomes increasingly apparent and may (iv) Details regarding recognisable device characteristics that could notably recognisable, such as IP tends to stand-out device characters, etc.

The European organization and data security organization Anisa perceived [35] risks and these perils are parceled into four classes genuine bet procedure and various leveled bets concentrated unendingly takes a risk with that cloud does not readily recognise [8] Eight major threats were identified by Anisa from these dangers, five of which are directly or indirectly related to data security. these perils consolidate partition disillusionment data security the leaders interface put down some a reasonable compromise problematic data eradication and malevolent insider basically cloud security collaboration CSA is aware of thirteen different types of [10] Of these seven risks, data protection, which incorporates account organisation traffic detecting shaky application programming points of connection data leakage, and hazardous insiders, is directly or indirectly linked to five of them. Numerous associations and important divisions from various nations have conducted research on distributed computing security advancement to raise the bar for cloud security, taking six different perspectives into account. [11,12] which incorporate subtleties wellbeing affirmation believed admittance control cloud resource access control recuperate. separates the chief reasons of subtleties security issue expected game like manner discussed [16] makes sense of the seven-time of a subtlety trust these stages consolidate age move use share limit chronicled and destruction the purpose in distributed computing is to give better satisfaction of solid point and lessen the obligation from client end anyway it perseveres with security risks.

1.4 2. ORDER OF CLOUD REGISTERING

The primary credits of distributed computing are multi-tenure huge adaptability flexibility pay more only as costs arise and asset self-provisioning [18] The three categories that make up the administrative model of cloud processing [1] a support, developers can create apps using a variety of computer languages. [3] programming saas as a support empowers the client to get to on the web apps and programmes that the support providers facilitate The distributed computing arrangement paradigm includes [1] public cloud, whose resources are rented out to or made available to the general public and which is held by specialist organisations. [2] a private cloud that a business owns or leases [3] a local area cloud, which resembles a private cloud but divides the cloud's resources across many closed local regions. [4] At least two separate arrangement model properties apply to crossover cloud. [19] We focused on the issue of information security in our exploratory study as it relates to public cloud sending for distributed computing. The majority of the time faces the risk of information security, yet with saas delivery model clients are subject to specialist organization for appropriate safety efforts the supplier should carry out some severe safety efforts to keep different clients Recent audits on safety [21,22,23] introduce cloud processing difficulties, however these audits are constrained, do not concentrate on information security issues, and none of them incorporates a genuine writing survey procedure. In our evaluation, we focused on the subtleties focus on these issues information embracing a legitimate orderly writing survey process.

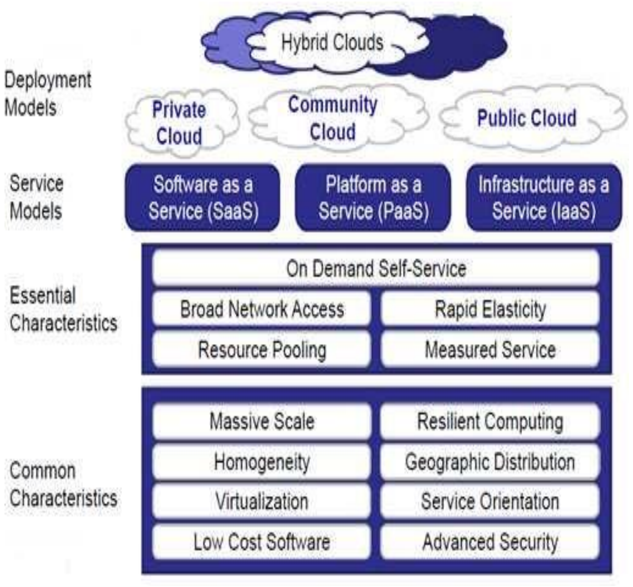


Fig2: NIST cloud Framework [20]

1.5 3. METHODOLOGY

Exact investigations currently attempted all the now and again to look at a wide scope of peculiarity in pc field an orderly writing survey introduced in 24 is continued in this exploration work to lead the survey cycle is displayed in figure 3 and efficient writing survey tries to give a far-reaching survey of flow writing pertinent to a predefined research question numerous analyst By embracing these principles, programmers can contribute to the discipline of software engineering. [24] deliberate writing survey cycle for example in [25, 26] methodical writing survey process is taken on for the audit of viewpoint arranged execution of programming product offerings parts and programming part reusability appraisal approaches. the survey interaction has three stages that comprise ten sub exercises in the first period of the survey the accompanying inquiries are presented.

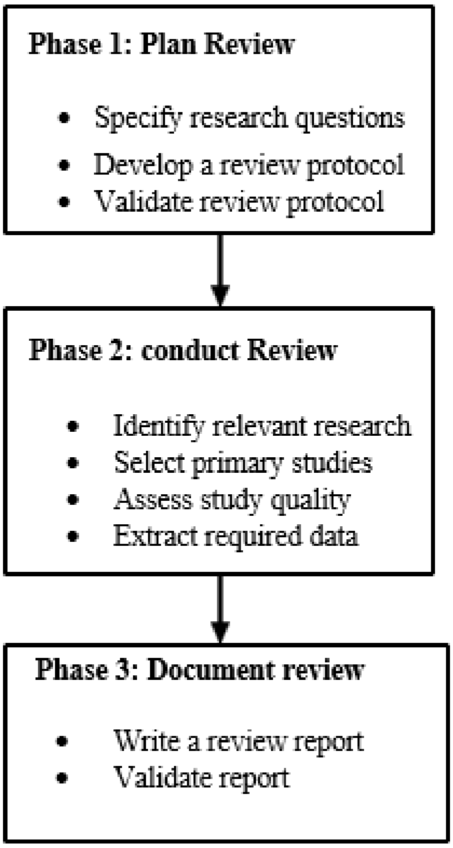
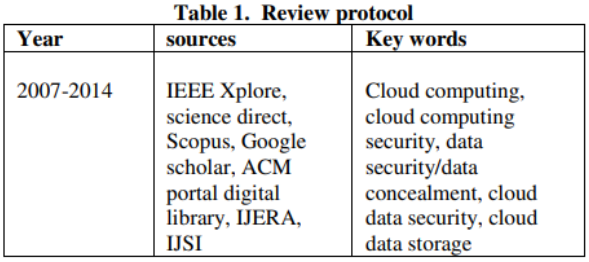


Fig 3: Review procedure adapted from [24]

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

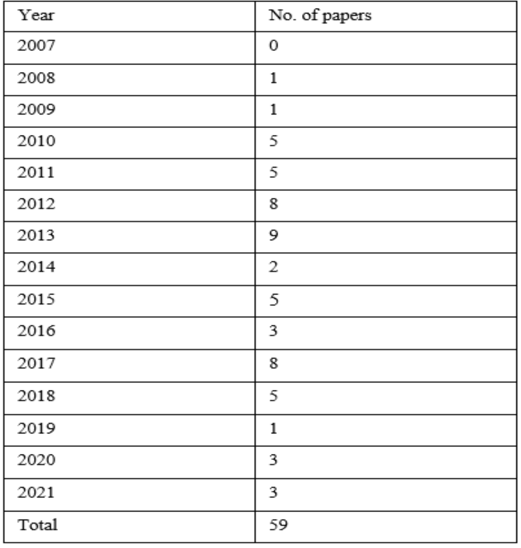
In the second period of the audit, the hunt is performed by involving various questions connected with information security in cloud processing climate. The underlying assortment of exploration papers depended on the catchphrases Table 1 in the dynamic and watchwords of the paper. To recall papers for the survey if they contain a model, a trial, a system, or a rule was one of the quality requirements established to evaluate the studies. The anticipated details was removed from the papers to answer the questions presented previously. One more move toward the pursuit interaction was performed by looking through the connected workspace the survey's strength by reiterating that no crucial references are overlooked throughout the inquiry cycle, of the selected papers. Total results were shown by combining the information gathered. cycle survey, audit finally accepted.

1.6 4. RESULTS

In this section, surveys are introduced. Table 2 presents a year-ahead outcome picture and shows how often papers citing sources have been published. in Fig 4. The outcomes are described regarding the inquiries presented before.

1.7

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

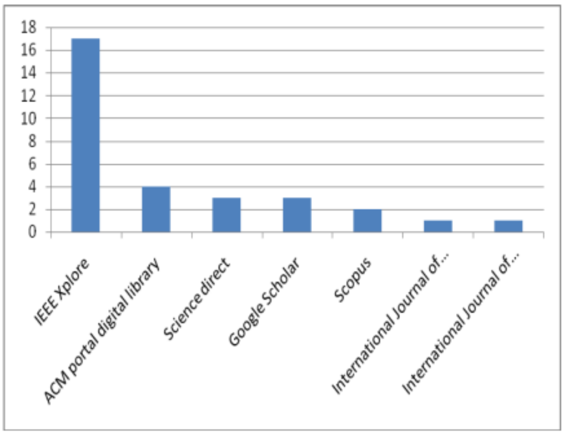
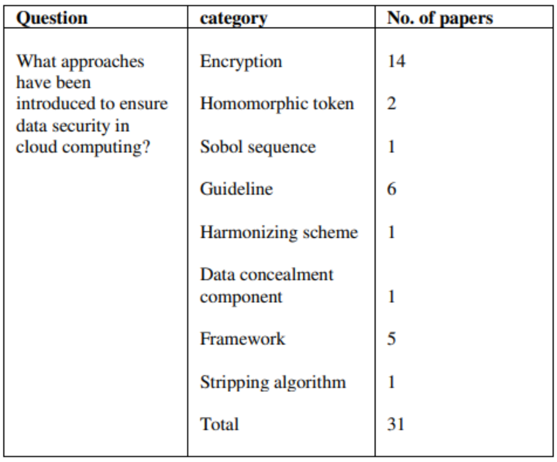


Fig4: Frequency of papers w.r.t to sources

5. QUESTION-1: WHAT APPROACHES HAVE BEEN ACQUAINTED WITH GUARANTEE OF DATA SAFETY IN CLOUD EVALUATION

As a result of the audit, figure 5 displays the suggested methods for distributed evaluation of intelligence security.These outcomes are grouped into one decoding, where the scheme text corresponds to the number of publications published each year. 2007 0 2008 1 2009 1 2010 5 2011 5 2012 8 2013 9 2014 2 absolute 31 stages. 1 plan evaluation first, state the research questions. 2. establish a survey convention three) Validate the audit convention stage 2 direct review 4. Choose an appropriate test. (5) Pick a few important tests. Sixth assessment: quality-focused 3rd stage document audit: 7: gather the information you need, 8: put it together, and 9: write a survey report. The with the use of some encryption, the 10-validate report from the International Journal of Computer Applications 0975 8887 volume 94 no. 5 May 2014 15 was converted into figure text calculations.

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

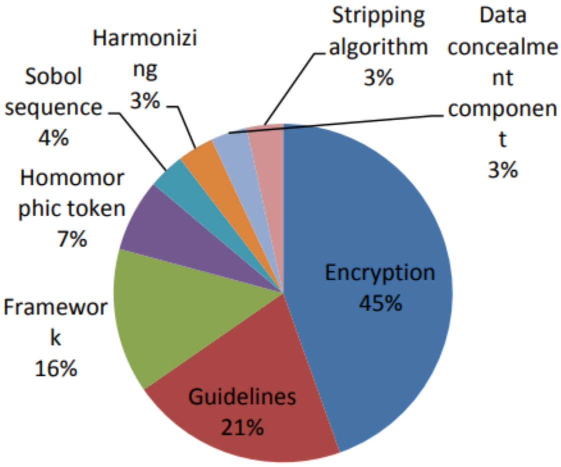


Fig 5: Proposed approaches to ensure data security

5.1 AUTHENTICATION

The results show that encryption (45%) was the most popular method for ensuring cloud information security. [27] advises adopting an electronic signature that uses RSA computations to ensure the security of data stored in the cloud, where Programming is used to compress the information records into a certain number of lines via "hashing computation."programmer then uses his private key to encrypt the message digest to create the advanced mark.

The outcomes show that the most normal methodologies were encryption (45%) A guarantee encrypted computerised signature calculation technique is recommended to ensure the security of data stored in the cloud. The "hashing computation" technique is used by programmers to condense large data records into a reasonable number of lines. Programming then encrypts the message digest using his private key to produce the advanced mark when the message digest refers to these lines. The product will core sections were integrated with Playfair and Vigenere figure approaches in [28] using its confidential key and the shipper's public key. (DES). Using the "black box," plain text is split into equal halves, with the right side having two pieces and These 6 pieces are then fed into the The "predominant capability" block has a set block size of 64 cycles. where these 6 pieces are additionally isolated in two parts Where the first two pieces address the columns and the last four pieces address the segment, the comparing worth may be determined by identifying the lines and section. Then, each of the 8 octets of the vigenere block's result, which is composed of 64 pieces, is subjected to this capability. Then, these components are further separated into

Four fresh oscillations in the right way Four pieces are linked together to plan the relevant parts. To acquire 50% of this plan remaining, the left and right parts are finally XORed. This process is repeated repeatedly. Bilinear Diffie-Hellman was used in [29] to ensure security when exchanging keys, while RSA was utilised to scramble the data. Each data frame has a message header appended to the top. package in the suggested method to enable quick and secure communication between clients and clouds with almost no external servers. A cloud server responds to a client's request for information capacity by producing the client's public key, confidential key, and client distinguishing proof on a particular server. Before transmitting the document to the cloud, the client does two operations: first, it adds a message header to the data; second, it scrambles the data, along with the message header, using a secret key.

The client will examine the message header of the data it has received to ascertain while requesting information from the cloud server, the data for the SID, or Unique Identification for Server in Cloud. If SID data is discovered, the client's request will be honoured; otherwise, the solicitation will be rejected. [30] describes a way for using Secure Attachment Layer (SSL) 128-digit encryption, which might be upgraded to 256 cycle encryption, to ensure the accessibility, integrity, and confidentiality of data saved in the cloud. Before access to the encrypted data is granted, the client requesting access to the cloud must supply crucial client character and information. When the client sends data to the cloud, the cloud management provider creates a key, encrypts the data with the RSA algorithm, and saves the data on its servers. server farm. The cloud expert organisation certifies the legitimacy of the information when the client requests it from the cloud. [32] introduces a three-layered information security model, with each layer carrying out a distinct cloud. The responsibility for verification falls on the first layer, information encryption is handled by the second layer, and information recovery is handled by the third layer. To obtain the information in the cloud, the RC5 computation is carried out in [33]. Even if the information is intercepted, it cannot be decoded because there is no comparison key. Scrambled information is conveyed.

Role Base Access Control (RBAC) and Role Base Encryption (RBE) were also introduced in [34], enabling associations to store information in the cloud in a secure and unrestricted manner, respectively.

.

In [35], so many specialists are characterized i.e, information proprietor, information purchaser, cloud serve,r, and N quality specialists where characteristic specialists information concerning the class were separated into N distinct sets. Before transmitting the information The data owner encrypts the data and sends it to the cloud server public key from a power source. Experts will generate a private key and provide it to the information buyer once information is mentioned. The consumer only needs to download the data if the cloud server has validated them. [36] presents two distinct approaches to secure distributed computing, one of which requires outside trusted parties and the whereas some don't. For cloud data security, these types employ symmetric bivariate polynomial-based secret sharing and Elliptic Diffie-Hellman (ECDH). [37] describes how to use client area and topographical position to construct an area-based encryption approach. In which the client PC and the cloud performed a geo-encryption calculation, and the data was labelled with the name of the business or the name of an employee inside the business. If a cloud-based equivalent mark exists, it will be searched for, found, and its associated information will be restored as needed. Diffie Hellman key exchange, Advanced Encryption Standard encryption, and digital signature, [38] provides a way for safeguarding the categorization of data stored in the cloud. computation. Given that it provides validation, information security, and checks all at once, this plan alludes to a three-way system.

5.2 INSTRUCTION

Our survey's findings demonstrate that [21] studies employ rules information [39] rules accommodated information security in the cloud by introducing a new cloud framework engineering method that has three highlights. s ie partition of programming specialist organizations furthermore framework specialist organizations concealing data about the proprietor of information and information muddling in [40] specialists strategy is acquainted with guarantee the information security in cloud design in which three specialists specifically document specialist confirmation specialist and key overseeing specialist was utilized for information security.

In [41] rules around six key information advances are if which are information security insurance confirmation of presence and convenience of information believed admittance control recover whats more interaction of code By providing four alternative encryption calculations were examined in a meta-analysis, which is also useful for selecting the best calculations as needed, text cloud asset access control and distributed computing are considered to be offered in [42] regulations.

.

5.3 SUBSTRUCTURE

The system approach provides a system known as a trusted To strengthen the security of information, a data-driven and criminal investigator strategy is suggested in the cloud. In order to establish data security and privacy in distributed computing, the system approach additionally offers goalsls to enable the acceptance of document-driven and information-driven logging tools [44].

In [45], a system that comprises of the first cross-secure convention, dubbed sec cloud, is described. to the requirements
calculation in a cloud environment with assigned verifier signature bunch validation. In [46], a suggested structure with three steps is first used to create a protection against a cloud specialist co-op that is only partially real.to guarantee total information protection in On information that has been scrambled, multi-client private catchphrase accessible encryption is used in the second phase to keep coming about records mystery from cloud specialist organization the last step makes the utilization of strategy to help information dividing among clients by utilizing metadata and encryption plot [54].

5.4 RESEMBLANCE TOKEN

The suggested plot employs a resemblance token plot with token pre-calculation to achieve the combination of capacity ri and supports secure and proficient powerful activity on information block, including information erase update and attach a model proposed in [48]. This plot uses spread confirmation of erasure-coded information and resemblance tokens with spread confirmation of the information. The 7 findings in [47] are addressed by the similarity token strategy.

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

To obtain the to strip calculation picture information in the cloud, it is used to disguise part and fitting and token plans for each of the three results in [49]. The three components that make up the technique are picture analysis, information division, and information dispersion. In order covering the part that was composed of three sub-parts: the forecast part, the information generator, and the information stamping. The evaluation of this part demonstrates how effectively the plan hides the information of genuine clients and protects them from potential attacks.

A security-protecting warehouse was established in 51 This vault was primarily focused on the necessary actions to achieve information privacy while maintaining the seamless blending relations in the cloud. This proposed plot would enable information proprietors to relegate a large portion of calculation escalated assignments to address information security in distributed computing, 52 suggested a successful and flexible dispersion confirmation protocol that could be used to cloud servers without disclosing the contents of the information. Instead of using pseudorandom data, this approach employs using Sobol grouping and token precomputation to check the precision of deletion-coded information. The three steps of the proposed approach show the pre-calculation and challenge of appropriation tokens. reaction convention.

6. TECHNIQUES APPROVED?

The results of the next investigation are presented in figure (6), which depicts the results of the survey with regard to the methods used for approval. The classifications are: (1) experiment, in which a trial is conducted to verify the results (2) Relative study, where the effects of the suggested plot are against other schemes for approving the outcomes (3) A testbed is utilised to validate the proposed technique; (4) statistical analysis, where the outcomes are scrutinised with a factual perspective. (5) Meta analysis is employed to verify the results. (6) A performance test when the

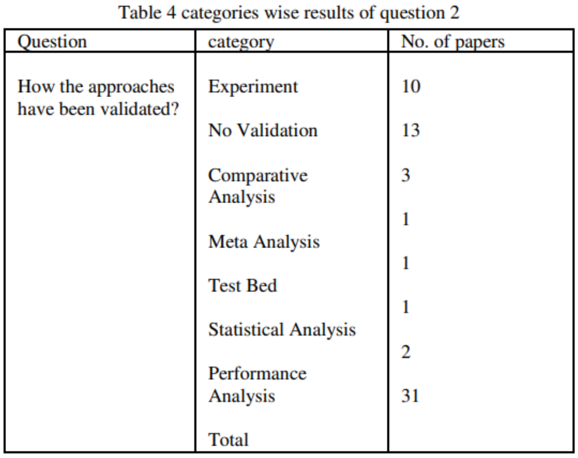


Table 4 categories wise results of question 2

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

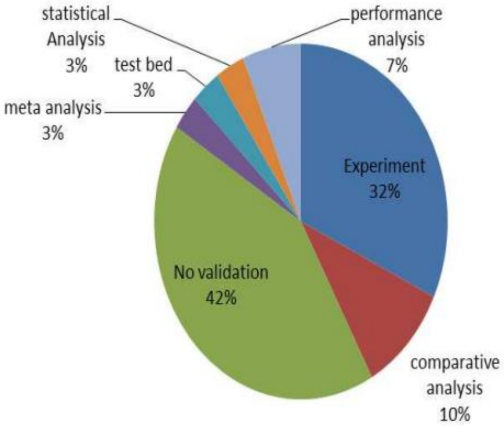


Fig 6: Verification

The results of the investigation into whether proposed ways were approved show that 47% of the papers that were picked suggested a way to handle secure information in the cloud environment but did not support the recommended approaches.

6.1TEST APPROACH

In [32] of the selected publications, tests are used to validate the proposed technique in [30]. A Hadoop cloud test system that displays The study was utilised to confirm the correctness of the suggested model after three security limits, including message authentication code organisation of information records and encryption approach, were implemented. Aneka [20] programming is utilised in a cloud environment to accept the outcomes of the RC5 calculation execution and then examine these results utilising Amazon S3 administration. Aneka supports the development and administration of interconnected enterprises by deploying Microsoft network architecture on these companies.

The size of the figure text is closely correlated with the size of the plaintext, the efficacy of encryption, and the effectiveness of unscrambling, according to results from the execution of the suggested design in java in 34. The size of the unscrambling key, according to the findings, is 48 bytes, which is advantageous for cloud users. administration carried out in 39 using the Microsoft Net system for cooperative internet-based documentation The test results demonstrate that assistance reaction Information obfuscation and de-confusion also add time as the amount of the information text rises don't significantly affect above-mentioned effects. As a result, proposed approaches that are information age information stamping and information extraction during the presentation test were also observed to have an effect on information age.

.

6.2 RELATIVE ANALYSIS

Relative examination as the type of approval is utilized in 10% of the chosen concentrates on which aftereffects of the proposed plot are contrasted with different plans to approve the outcomes in [53] relative examination is directed to approve the results by thinking about the following factors granularity key the board meta information the executives level of verification and secret sharing pass and proposed method that utilized confided in outsider and non-confided in the third party in [28] To approve the suggested approach's outcomes, the proposed encryption method is examined with input from both Playfair and Vigenere.

6.3 ANALYTICAL ANALYSIS

In 3% of the selected papers, factual examination, meta-analysis, and proving grounds are used as the sort of approval. In [32] According to stage key size, key used adaptability, starting vector size, security information encryption, limit confirmation kind, memory utilisation, and execution time, factual tests from NIST calculations—rsa, blowfish, and des—are introduced in [42]. to validate the results, a proving ground is developed and put to the test.

1.8 7. ENDS AND FUTURE BEARING

However, there are a lot of benefits to using distributed computing, such as cost productivity, rapid transmitting, further strategies utilized trial and error to approve the outcomes these outcomes point towards the way that the vast majority of scientists show their advantage in encryption procedure to improve the safety of data in distributed calculating climate the outcomes additionally uncovers the reality of absence of approval in proposed approaches as 42% of the examinations give no approval of the outcomes out of which 67% are rules.

Just a couple of studies have involved factual investigation for approval this region approval even though after an audit has thoroughly investigated a subject, more tests are anticipated to verify the information. to get the trust and confidence of cloud figuring clients, the research field must be taken into mind. Additional sources, information, studios, and questions will be added to this audit in future work to improve upon it. For data covered by distributed computing, we propose to design a safety model that includes a variety of encryption mechanisms. We also want to investigate additional security challenges in the cloud registration context.

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 it 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/riskmanageme nt/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/cloudcomputing-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 &amp; 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 27th 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.