*i*Journals: International Journal of Software & Hardware Research in Engineering (IJSHRE)
ISSN-2347-4890
Volume 9 Issue 1 January 2021

A Review on Data Security in Cloud Computing

Dr. Keshao D. Kalaskar[1], Ms. Shipra Yadav[2] and Dr. Pankaj Dhumane[3]

[1]Associate Professor, Dr. Ambedkar College, Chandrapur, (MH), India,
keshao_kalaskar@yahoo.co.in

[2]Research Scholar, IICC, RTM Nagpur University Nagpur, (MH), India,
shiprayadav621@gmail.com

[3]Assistant Professor, Sardar Patel College, Chandrapur, (MH), India,
pdhumane@rediffmail.com

ABSTACT

Cloud computing is an Internet-based computing and next stage in evolution of the internet. It has received significant attention in recent years but security issue is one of the major inhibitor in decreasing the growth of cloud computing. It essentially shifts the user data and application software to large datacenters i.e, cloud, which is remotely located, at which user does not have any control and the management of data may not be completely secure. However, this sole feature of the cloud computing introduce many security challenges which need to be resolved and understood clearly. One of the most important and leading is security issue that needs to be addressed. Data Security concerns arising because both user data and program are located in provider premises. In this study, an attempt is made to review the research in this field. The results of review are categorized on the basis of type of approach and the type of validation used to validate the approach.

Keywords

Data security, cloud data concealment, cloud security, review

1. INTRODUCTION

Cloud computing is an emerging technology which recently has drawn significant attention from both industry and academia. It provides services over the internet, by using cloud computing user can utilize the online services of different software instead of purchasing or installing them on their own computers. According to the National Institute of Standard and Technology (NIST) definition, cloud computing can be defined as a paradigm for enabling useful, on-demand network access to a shared pool of configurable computing resources [1]. According to Gartner [2] cloud computing can be defined as a style of computing that delivered IT capabilities 'as a service' to end users through internet.

According to recent survey by International Data Group (IDG) enterprise, the top three challenges to implementing a successful cloud strategy in enterprise vary significantly between IT and line-of-business (LOB). For IT, concerns regarding security is (66%) and 42% of cloud-based projects are eventually brought back in-house, with security concerns (65%) [3]. A survey conducted by International Data Corporation (IDC) in 2011 declares that 47%

IT executives were concerned about a security threats in cloud computing [4]. In survey conducted by Cisco's CloudWatch 2011 report for the U.K. (research conducted by Loudhouse) 76% of respondents cited security and privacy a top obstacle to cloud adoption [5].

Data security is a major concern for users who want to use cloud computing. This technology needs proper security principles and mechanisms to eliminate users concerns. Most of the cloud services users have concerns about their private data that it may be used for other purposes or sent to other cloud service providers [6]. The user data that need to be protected includes four parts [7] which are: (i) usage data; information collected from computer devices (ii) sensitive information; information on health, bank account etc. (iii) Personally identifiable information; information that could be used to identify the individual (iv) Unique device identities; information that might be uniquely traceable e.g. IP addresses, unique hardware identities etc.

The European Network and Information Security Agency (ENISA) identified thirty-five risks and these risks are divided into four categories: legal risk, policy and organizational risks, technical risks and risks that are not specific to cloud [8]. From these risks, the ENISA identified eight most important risks. Out of which five risks concerns directly or indirectly related to the data confidentiality. These risks include isolation failure, data protection, management interface compromise, insecure data deletion and malicious insider. Similarly, The Cloud Security Alliance (CSA) identifies the thirteen kind of risks related to the cloud computing [9]. Out of these thirteen risks CSA declares seven most important risks [10]. Five of these seven risks are directly or indirectly related to the data confidentiality which includes: account service, traffic hijacking, insecure application programming interfaces, data loss/leakage and malicious insiders.

Different countries, IT companies, and the relevant departments have carried out the research on cloud computing security technology to expand the security standards of cloud computing. Existing security technology reflected in six aspects[11,12] which include: data privacy protection, trusted access control, cloud resource access control, retrieve and process of cipher text, proof of existence and usability of data and trusted cloud computing. To enhance the data security the data can be converted into cipher text but this may cause to lose many features when data is converted into cipher text.

There are two widely used methods to retrieve the cipher text. First, there is a safety index-based approach which establishes a secure cipher text key words indexed by checking the existence of key words [13]. Second, there is a cipher text scanning-based approach which confirms the existence of key words by matching each word in cipher text [14]. [15] Lists the top ten obstacles in the popularity of cloud computing. The data security and storage issues is discussed in this article and it also analyzes the main reasons of data security issue, possible solutions of this issues and some future development of cloud computing are also discussed. [16] Explains the seven phase of data life cycle in cloud computing that also need security to get user trust these phase include; generation, transfer, use, share, storage,

archival and destruction. The aim of cloud computing is to provide better consumption of resources and reduce the work load from user end but it suffers with security threats [17]. The complexity of security in complete cloud computing environment is shown in figure 1.

In figure 1 the lower layer indicates the deployment models of cloud computing namely private cloud, community cloud, public cloud and hybrid cloud. The layer just above the deployment model represents the services delivery model of cloud computing. These service delivery models exhibit the certain characteristics that are shown in the top layer. These fundamental elements need security with respect to the characteristics of selected deployment model. Some of fundamental security challenges are shown in the vertical layer given in figure 1.

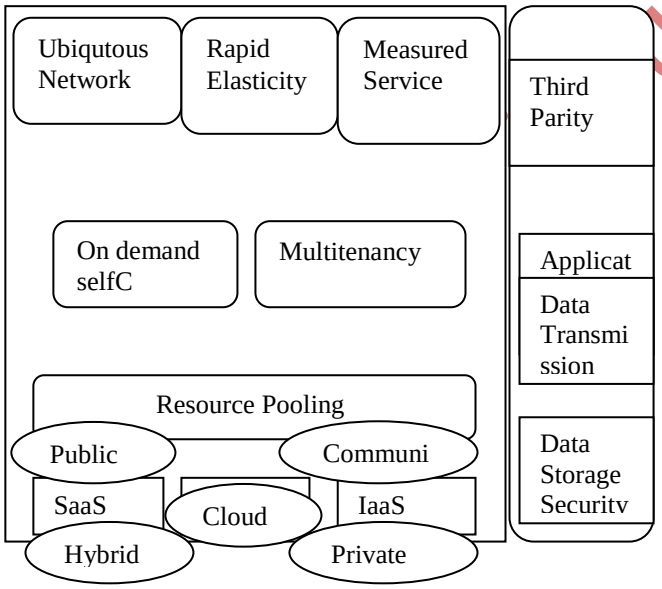

Figure.1 Complexity of security in cloud environment [21]

2. CLASSIFICATION OF CLOUD COMPUTING

The main attributes of cloud computing are Multi-tenancy, massive scalability, elasticity, pay as you go and self- provisioning of resources [18]. The services model of cloud computing is divided into three categories (1) IaaS (infrastructure as a service) provides the use of virtual computer infrastructure environment, online storage, hardware, servers and networking components; (2) PaaS (plat form as a service) provides platform for developing applications by using different programming languages; (3)

SaaS (software as a service) enables the user to access online applications and software that are hosted by the service providers. The deployment model of cloud computing include (1) public cloud, that owned by service provider and its resources are rented or sold to the public (2) private cloud, required data was extracted from the papers to answer the questions posed above.

that is owned or rented by an organization (3) community cloud, that is similar to private cloud but cloud resources is shared among number of closed community (4) hybrid cloud, exhibits the property of two or more deployment models [19]. Figure 2 shows the NIST definition framework for cloud computing.

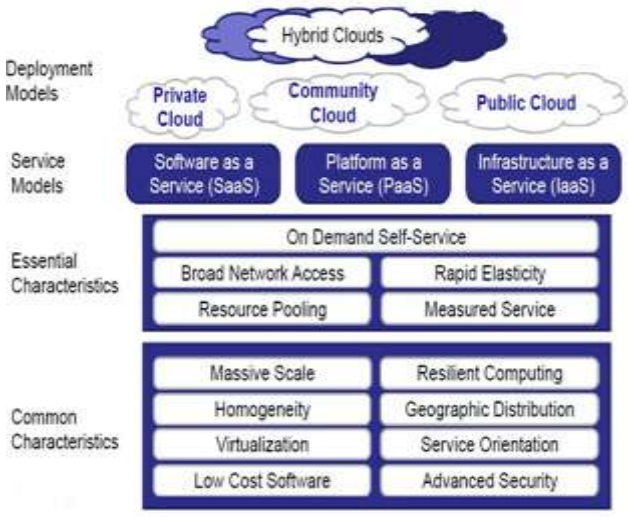

Figure.2 NIST Cloud definition Framework [20]

In this research work we focused on data security issue in Cloud Computing Environment. Public Cloud Deployment Model mostly suffer from the risk of data security. On the other hand in SaaS delivery model client is dependent on service provider for proper security, measures. The Provider must implement some strict security measure to keep multiple user from seeing each other's data and gain the trust of users. Recent Review on security issues in Cloud Computing are presented in [21,22,23] but theses review are limited and not focused on detail study of data security issues. Neither of them adopt a proper literature review process. In Our study we focused on details study on data security issue by adopting a proper systematic literature review process.

3. METHODOLOGY

Empirical studies are now being undertaken more frequently, as a means of examining a broad range of phenomenon in computer field. A systematic literature review presented in[24] is followed in this research work to conduct the review.

The review process is shown in figure 3. A systematic literature review endeavor to provide a comprehensive review of current literature relevant to a specified research questions. Many researchers contribute their efforts in the field of software engineering/computer science by adopting [24] systematic literature review process such as in [25, 26] systematic literature review process is adopted for the review of aspect oriented implementation of software product lines components and software component reusability assessment approaches.

Required data was extracted from the paper to answer the

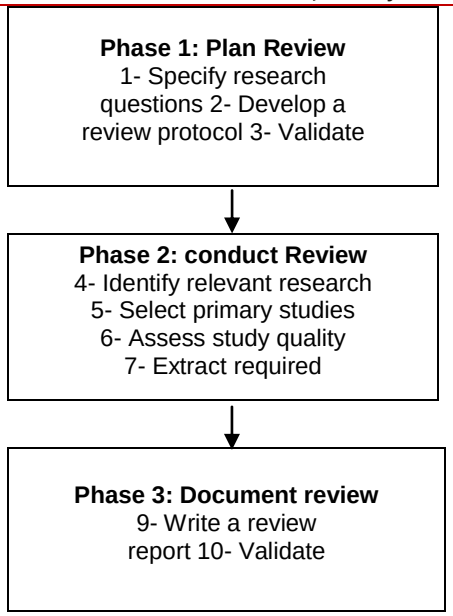

Figure.3: Adapted review process from [24]

The analysis mechanism comprises of three stages, comprising of ten sub-activities. The below concerns are presented during the first process of the evaluation:

Question 1: "WHAT APPROACHEs HAVE BEEN INTRODUCED TO ENSURE DATA SECURITY IN CLOUD COMPUTING?"

Question 2: "HOW THE APPROACHES HAVE BEEN VALIDATED?"

The concerns are posed during the first step 1 sub-activity, a review procedure has been established. The analysis procedure shall contain the references, the time span under review and the main terms included. This procedure is revised and checked after certain improvements have been made by the researchers. The procedure for the final analysis as seen in Chart 1. References used in this analysis involve "Science Direct, IEEE xplorer, Google scholar, Scopus, ACM public library portal. In addition, we looked at JCMS, the IJSI papers. The study focuses on the duration from 2007 to 2014."

Table.1: Review Protocol

Year	Source	Keyword
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 next step of the analysis, separate data protection questions in the cloud storage setting would be used to scan. The original selection of research articles was focused on the keywords in Table 1 of the reports, keywords and abstracts. The consistency standards established for the appraisal of the studies is to include the documents in the analysis if the necessary details were retrieved from the articles in order to address the questions presented earlier.

4 RESULTS

The findings of the examination shall be discussed in this portion. The reason for the year is illustrated in Table 2 and the intensity of the documents with regard to the references is illustrated in Fig 4. The findings are defined by the concerns presented earlier.

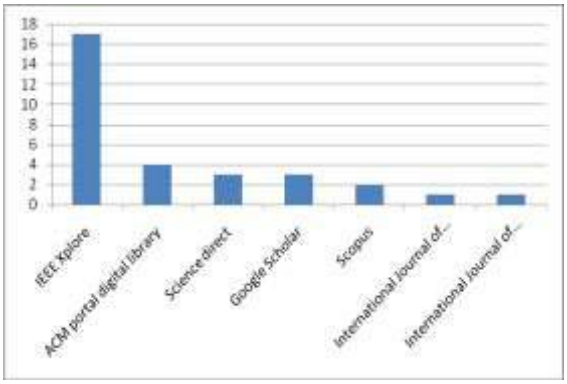

Figure.4: Frequency of papers wrt sources

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
Total	31

5. QUESTION-1: WHAT APPROACHES HAVE BEEN INTRODUCED TO DATA SECURITY IN CLOUD COMPUTING?

The analysis results (Figure 5) indicate the suggested methods to cloud storage data protection. Those findings are clas0sified as: (1) encryption by way of such encryption algorithms where the simple text is translated into cypher text; (2) homomorphic token. A methodology means that the data analysis key does not need to be decrypted but that we may evaluate the encrypted symbol explicitly; (3) guidance. Some reports have described a range of cloud data management guidelines; (4) harmonization framework Constructing a data repository; (5) a data concealing component; (6) a token; (7) a framework; (8) a stripping algorithm.

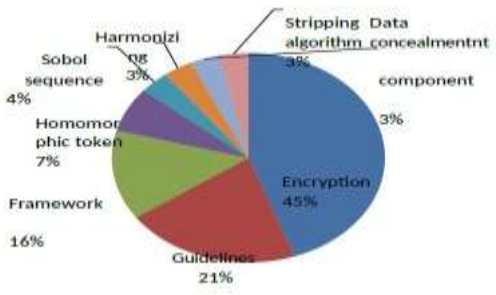

Figure.5: Proposed approaches to ensure data security

Table.3: Category wise results of question 1

Questions	Category	No of Papers
What pproaches have been introduced to ensure data security in Cloud Computing/	Encryption	14
	Homomorphic token	2
	Sobel Sequence	
	Guideline	1
	Harmonizing Scheme	6
	Data Concealment component	1
	Framework	1
	Stripping	5
	Algorithm	1
	Total	31

Generation was observed.

Encryption

The findings indicate that the greatest feasible strategy is encryption (45%) to maintain cloud data protection. In [27] an RSA-based digital signature to guarantee the confidentiality of the data in the cloud is suggested. In which programme the data records are cropped down in a few lines of "algorithms." These lines are named "message digest" and the programme then verifies the "message digest" to create the digital signature using a privately owned key. The softws with their own secret key and shared recipient key will decode the digital signature into "message digest." In [28] Playfair and vigenary cipher methods have been coupled with the structural elements of the "Simplified Data Encryption Standard (SDES) and Data Encryption Standard (DES)." "In which 64-bit block size of plain text is taken which is fixed and this 64-bit plain text is divided into two halves by using the 'black box' the right half have 2 bits whereas left half has 6 bits, then these 6 bits are feed into 'superior function' block where these 6 bits are further separated in two halves where first two bits represent the rows and last four bits represent the column by identifying the rows and column the corresponding value can be selected. Then this function is applied to all 8 octets of the output of vigenary block the resultant of black box is again of 64 bits then these bits are further divided into 4 new octants similarly right 4 bits are unified to formulate right halves. Finally, left and right halves are XOR-ed to obtain left half of this arrangement.

This process is repeated three times. "In [29] "The RSA algorithm used to encrypt the data and the Diffie-Hellman Bilinear algorithm" guarantees confidentiality during key exchange. For clear and secure contact among computer and cloud without even a third party server, a "message header" shall be attached to the developed framework. "When user sends the request to the cloud server for data storage then cloud server creates the user public key, private key and user identification in certain server." Until submitting the file to the cloud, two activities are performed at user end, first add a "message header" and then encrypt the files with "message header" using a hidden key. When you submit data from users to the cloud service, the message header searched for obtained data and retrieved "Server in cloud (SID) information" details in the cloud. The user's request would otherwise be lowered if SID knowledge is identified.

In [30], a strategy is adopted to guarantee the accessibility, confidentiality and anonymity of cloud-based data utilizing "Secure Socket Layer (SSL) 128-bit encryption," which can also be improved to "256-bit encryption." Users attempting to retrieve information to the cloud are specifically necessary to have valid user identification and

passwords prior to accessing the encrypted information. In [31], the user transfers the information to the computer and then creates a cloud service provision and verifies the customer data using an RSA algorithm. As the consumer demands data from the cloud, the cloud service company can validate the identity of the user and supply the user with encrypted data which can be decoded by measuring the secret key.

The findings indicate that encryption (45 percent) was the most common form of maintaining data protection in the cloud. In [27] an RSA-based digital signature to guarantee the confidentiality of the data in the cloud is suggested. In which programme the data records is cropped back in a few lines of "hashing algorithm".A three-layer data protection paradigm is introduced in [32], whereby each layer executes various roles to keep data safe in the cloud. Initial layer is liable for authentication, signatures with an RSA algorithm system was suggested to guarantee data protection in the network. Wherein machines used "hashing algorithm" to break down data records in a few lines. "These lines are called message digest then software encrypts the message digest with his private key to second layer performs the duty of data encryption and third layer performs the functionality of data recovery." In [33], the "RC5 algorithm" is used to encrypt data in the cloud. Encrypted data is distributed and though the data is compromised, no equivalent key can be required to retrieve the message. It is suggested in [34] "Role Base Encryption (RBE)" technology to protect data in the cloud and "Role Base Access Control (RBAC)" cloud infrastructure to enable organizations to store data safely in the public cloud whilst retaining confidential organizational framework details in the private cloud.

In [35], four security services are identified, i.e. "the data owner, the data user, the cloud server and the N attribute authorities, where the attribute authorities set were divided into N disjoint sets for the group."The data holder collects the public key from each government and encrypts the data until they are transferred to the cloud server. As data is submitted, the authorities will generate a secret key and give it to the data user, and the customer will only be allowed to retrieve the file until it is checked by a cloud service. Two forms of secure cloud storage are suggested in [36], one involving trustworthy third parties and the other not. These forms use "Elliptic Curve Diffie-Hellman (ECDH)" and symmetrical bivariate hidden sharing dependent on polynomials to maintain data confidentiality in the cloud world. Site-based encryption technologies utilizing device location and geographical place has been implemented in [37]. In which a "geo-encryption algorithm" was applied on the cloud and user device, as well as the data was labelled with the company name or individual employed in the organisation. Once data is needed, a related mark will be checked and recovered in the cloud and the details referring to the label will be extracted. A strategy is suggested in [38] utilizing "digital signature and Diffie Hellman key exchange" in conjunction with "Advanced Encryption Standard encryption algorithm" to secure the secrecy of data processed in the cloud. This system is alluded to as a three-way process since it offers at the same time authorization, data protection and confirmation.

5.2 Guidelines

The results from our study indicate that 22% of study results use cloud data security standards. [39] offers recommendations for cloud data management by implementing a modern cloud design approach with three features: isolation

between database and technology service providers, knowledge concealed from data owner and data obscurement. In [40], a data protection approach in the cloud infrastructure is implemented by department. With data security three agents - "file agent, authentication agent and key managing agent" - were used. [41] provides guidance on six main data technology: "data privacy protection, proof of existence and usability of data, trusted access control, retrieve and process of cypher text, cloud resource access control and trusted cloud computing." In [42], criteria are set by the meta-analysis of four different encryption algorithms, which help to choose the right algorithms as appropriate.

5.3 Framework

14% of the findings come from the system strategy. A concept named "Trust Cloud"[43] aimed at improving data protection, seeking to facilitate implementation of a file-centric and data-centered logging system for the security and privacy of data stored in the cloud. The intent of this structure is to enhance the security and confidentiality of data. In [44], the construction of a multi-tenant structure offers a foundation. Where a strategy is created, it is divided into 3 levels, i.e. "layer, logic and access to data." These layers give user data pretty strong protection. The offers a structure consisting of the “SecCloud protocol”, a first protocol covering protected saving and stable cloud hosting via the specified verification signature and batch access control, sampling methods in deterministic terminology. In the suggested structure includes three phases, with the first step being taken precautionary to offer full data security to semi-honest suppliers of cloud services through indexing data and metadata. Searchable protection is achieved on secure data in the second process of multi-users, which prevents queries and the subsequent cloud storage provider's files secret. End of the policy to facilitate data sharing among users through the use of metadata and encryption.

5.4 Homomorphic Token

7% of the outcomes are expressed by the "homomorphic token" method. In the token scheme, "homomorphic data" protection schemes are implemented. The scheme suggested uses "homomorphic token" with disbursed erasure-coded authentication. It facilitates stable and effective data block dynamic activity including data deleting, upgrading and annexation. In a model suggested using the "homomorphic token" method with token recalculation algorithm is used to combine storage consistency insurance with abusing server recognition.

5.5 Harmonizing,data concealment component, Stripping algorithm, and token scheme

Each of the findings reflects 3 per cent of the "Stripping algorithm, data concealment component, and harmonizing and token scheme" Striping is used to protect the information data in the cloud through three modules: image processing, data isolation and data delivery. Architecture of the component concealing the data component consists of three sub-components: "the prediction component, data generator and data marking to secure the data in cloud." The assessment of this element demonstrates that legal users have effectively concealed data to defend them from possible attacks. As a privacy protection repository presented in the repository centered primarily on harmonizing activities, while retaining intact cloud harmonization relationships. This suggested scheme allows the data owner, without discovering data contents, to delegate most computer-intensive activities to cloud servers.

Introduced a protocol to validate the delivery reliability and accessibility for the management of cloud data protection. This protocol uses sobol pre-call tokens to validate the credibility of erasure-coded data rather than pseudo-aligned data. The model suggested consists of three phases: file delivery, pre-calculation tokening, and challenge answer protocol.

6 QUESTION-2: "HOW THE APPROACHES HAVE BEEN VALIDATED?"

Here you can find the results of the second question. The results of the assessment on the validation procedures are shown in Figure 6.The

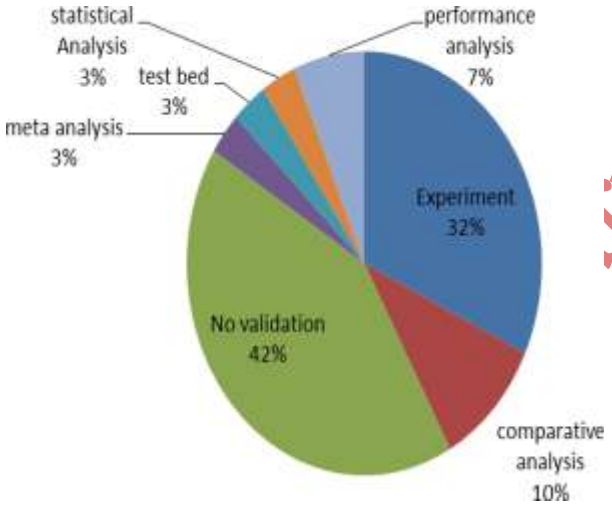

Figure.6: Type of validation

classifications are: "(1) Experiment, where an experiment is carried out to validate the results; (2) Comparative analysis, where the results of proposed scheme is compared to other schemes to validate the results; (3) Test bed is used to validate the proposed approach; (4) Statistical analysis, where the results are analyzed by using some statistical technique; (5) Meta- analysis is is used to validate the results: (6) Performance analysis, where the performance of proposed approach is analyzed by different methods; (7) Some of the proposed approaches have not performed any validation."Table 4 shows the specifics of the group and Figure 6 shows the percentage type of validity. Let the word validation be clarified. This applies, in addition to the demonstration/application of the technique suggested, to every scientific tool used as proof.

Table.4: categories wise results of question 2

Questions	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 findings of the issue on the justification of the suggested alternatives reveal that 48% of the chosen articles suggested a framework for data protection in the cloud world but do not include a justification of the suggested technique.

6.1 Experimental method

In 32 percent of chosen papers, evaluations are conducted to test the suggested method. The test was carried out with the aid of a cloud simulator called Hadoop to determine the feasibility of the proposed framework. It displays the security status following the introduction of three security criteria, namely: "Message Authentication Code, Data Classification, Index and Encryption Technique." In Aneka 2.0 programme is used in the cloud

setting to verify the findings obtained by applying the RC5 algorithm and then equate these results with the Amazon S3 service. Aneka makes it easy to create and operate an integrated network utilizing Microsoft.NET applications on these networks. The new structure is developed in Java in and the findings indicate that the text size of the cypher is sequentially comparable to the magnitude of the clear text as well as the performance of the encrypting and decrypting is quite strong. The findings also reveal that the cipher text key size is 48 bytes, that are user-friendly. C# Microsoft.NET system for shared online documentation is included in cloud services. The interesting new findings demonstrate that the service response time rises in a linear fashion as the value of the input texts improves and the obfuscation and de-obfuscation data do not create any overhead, which is why the suggested solution has shown practical efficiency. In the PHP language is being used for an analysis where an output test is performed for three phases, namely data creation, data labelling and data extraction. The component's effect on data generation was however examined during the output test.

6.2 Comparative study

Comparative analysis as a method of verification is used in 10% of the chosen experiments in which the findings of the present scheme are contrasted with other testing procedures. In comparative analysis the findings are checked by taking into account grit, main control, meta data management, concealment, delivery and execution standard, in compliance with the variable's granularity. The comparative analysis is rendered around data "Privacy by Authentication and Secret Sharing (PASS)" and the suggested methodology utilized by trusted third parties and non-trusted third parties. In the proposed encryption method is contrasted with the "DES, SDES, Playfair and Vigenere encryption" strategies used to verify the proposed solution performance.

6.3 Review of results

Quality review is used to verify the proposed method in 7% of the chosen articles. In performance review is carried out in terms of reliability and productivity to prove that the findings are verified, and the proposed system is extremely robust and efficient towards Byzantine failure and malicious code manipulation assaults.

6.4 Quantitative review

Data analysis, meta-analysis and testing platform as a method of validation was used in 3% of the chosen research. The NIST predictive test is used to verify the findings by choosing eight modern encryption algorithms. In a meta-analysis of four different protection algorithms that are "AES, RSA, blow fish and DES" is provided in terms of network, "key size, key used, scalability, initial vector size, security, data encryption capability, authentication sort, memory use and execution time to confirm the findings." The test bed is built and checked for confirmation of findings .

7 CONCLUSIONS AND FUTURE DIRECTIONS

There are several advantages to utilizing cloud infrastructure, such as cost effectiveness, fast implementation, increased usability, etc. Even so, there are many other realistic issues that need to be overcome. The security of data is one of them. Most researchers have contributed their measures to limit the problem of data protection in this area with the numerous solutions mentioned in this work. A systematic review was carried out on the work in the field of the protection of cloud storage data and the findings are discussed in this article. The findings reveal that the plurality of methods

are focused on encryption (45 per cent) of which 72 per cent of encryption strategies are validated. 67% of the encryption methods used research and testing to verify the findings. These findings point to the fact that most researchers are involved in encryption technologies to improve data protection in the cloud storage world. The findings further show the lack of consistency of the suggested methods, as 43 per cent of the experiments do not have justification of the findings where its 66 per cent are recommendations. Just a few researchers have utilized mathematical analysis for validation purposes. This field (validation) requires the focus of the testing community to create the trust and support of cloud infrastructure consumers. While our study examined the area, more research is required to validate the findings achieved. Future study involves the continuation of this analysis by adding a variety of references (conferences, articles and workshops) and queries. The future strategy is to explore other security concerns in the cloud computing world, and we also hope to build a protection model utilizing certain encryption methods for cloud computing data concealment.

8. 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- efinition.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-know- cloud- computing- Security (Accessed 23 December2013).

3] IDG Cloud Computing Survey: "Security, Integration Challenge Growth", [online]http://www.forbes.com/sites/louiscolumbus /2013/0813/idg- cloud-computing-survey- (Accessed: 28December 2013).

[4] Ricadela, "Cloud security is looking overcast"[online] http://www.businessweek.com/magazine/cloud-security- 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/cloud- computing/200657/only- seven-percent-uk-it- services-cloud-says- surveyS. (Accessed: 29December 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,"

[8] European Network and Information Security Agency (ENISA)"Benefits, risks and recommendations for information security"[online]http://www.enisa.europa.eu/activit ies/riskmanageme nt/files/ deliverables/cloud-computing- risk- assessment. (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," inCloud 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 /EECS2009-28.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]mall peter and Grace Tim" Effectively and securely using the cloud computing paradigm"

[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

[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, 28- 30 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), 1831-1838.

[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, Issue4.

[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 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 Asia- Pacific 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),1922-1926.

[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 Cloud Computing

[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

[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),

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

53] Anane, R., Dhillon, S., & Bordbar, B. (2008). Stateless data concealment for distributed systems. Journal of Computer and System Sciences, 74(2),243-25