

**DATA-CENTRIC PROTECTION IN INTER CLOUD ENVIRONMENT: A SURVEY**

Megha Vashishtha
PhD Scholar
Mewar University, Rajasthan, India

Dr. Pradeep Chouksey
Vice-Principal & Associate Professor
Computer Science, TIT, Bhopal, Madya Pradesh, India

Dr. Vivek Tiwari
Assistant Professor
Computer Science, IIIT-NR, Raipur, C.G., India

Abstract: Just about 70% of the organizations are right now utilizing or wanting to utilize Cloud Computing, being the capacity to convey more adaptability to the business by means of cloud offerings and diminished equipment and staffing expenses, the principle motivations to embrace Cloud Computing. Data sharing along with the resources can be easy to handle and adopt in the cloud. But this adaptability also alarms the security breaches "Is the data safe". So, security is a noteworthy concern now days. In this paper we have concentrated on data security based on data centric approach. For this reason, we have studies and suggest the analysis. The analysis is also supported by the previous outcomes.

Keywords: Cloud Computing, Data Security, Saas, Paas, IaaS

1. INTRODUCTION

Cloud computing is a procedure of figuring resources as a utility on interest [1-3]. This handling model will decrease the candid expense for making and sending information on the Internet. In such an area, resources can scale down and scale up quickly, thus under-provisioning and over-provisioning be a critical danger to organizations in the cloud model [4]. Distributed computing has grown as a champion amongst the most certain and asking for advancements of our time [5-8]. This new model uses two diverse inventive change utility enlisting and organization arranged building configuration to give the customers with amazingly versatile, pay-per-use, the whole thing as-an organization model for Information Technology (IT) movement [9-12]. It perceives the disseminated figuring organization transport model are flexibility/versatility, on-interest organization provisioning, essential resource pooling, multi-inhabitation encouraging, utility pay-as-you-use esteeming and thought of not very impressive layers [13]. The security concern is additionally major portrays which can be examined as in [14-16].

The cloud computing system depends on the layers for information transportation. The three fundamental administration layers that contain the distributed computing construction modeling in light of which the on-interest administration will be provided [15]. As indicated by [15] Software as a Service (SaaS) has changed desktop-based programming applications into online programming items that can be utilized around the world. In [15] suggested customer relationship management (CRM) for the client and server organization [15].

Keeping in mind the end goal to take care of the issue of information trustworthiness checking, numerous plans are proposed under distinctive frameworks and security models [16-22]. In every one of these works, incredible endeavors are made to plan arrangements that meet different necessities: high plan proficiency, stateless confirmation,

unbounded utilization of questions and irretrievability of information, and so on. At that point, customers have the capacity to appoint the assessment of the administration execution to an autonomous outsider evaluator, without commitment of their calculation assets. Accordingly, for pragmatic utilization, it appears to be sounder to furnish the check convention with open auditability, which is relied upon to assume a more imperative part in accomplishing economies of scale for Cloud Computing. Besides, for effectiveness thought, the outsourced information themselves ought not to be needed by the verifier for the check reason. Different other approaches are also suggested in the direction of cloud security have been presented in [23-30].

2. RELATED WORK

In 2012, S.U.Muthunagai et al. [31] proposes a novel structural planning Efficient Cloud Protection System (ECPS) which recognizes the visitor to-visitor assault in the Virtualization environment and gives proficient access of cloud assets to the clients by giving simple access to the ordinarily utilized assets that spares the time spent in getting too much of the time utilized assets. This structural engineering will incorporate the elements of cloud security parts like interceptor, cautioning recorder, and so on. To decrease the processing in this way upgrading the security of the cloud assurance framework.

In 2012, Mohammed A. AlZain et al. [32] recommend that the security gets attentiveness toward information classified, notwithstanding respectability and accessibility. Security has the qualities of a supplement to dependability. They propose another model called Multi-Mists Databases (MCDB) which utilizes multi-mists rather than single cloud administration supplier, for example, in Amazon cloud administration. Their proposed model likewise joins the Shamir's mystery sharing methodology. Furthermore, it receives a triple secluded repetition (TMR) strategy with

successive technique to enhance the proposed distributed computing system reliability and after that improve the security viewpoint.

In 2012, Yun Yang *et al.* [33] highlighting the significance of distributed computing in the improvement of savvy network. As per the qualities of savvy brace, the key innovation and examination point is shown in the paper of late. They suggest the security preview on mass information security in insightful network.

In 2012, AshutoshDubey *et al.* [5] proposed a proficient technique for information revelation which is in view of subset and superset approach. In this methodology they additionally utilize dynamic least bolster with the goal that we diminish the execution time. A successive superset implies it contains more exchanges than the base backing. It uses the idea that if the thing set is not visit but rather the superset may be visit which is consider for the further information mining errand. By this methodology we can likewise discover enhanced affiliation, which demonstrates what thing set is most adequate relationship with others. A continuous subset implies it contains less exchanges than the base backing. It uses the conduct that the less check may be visit on the off chance that we appended the less tally with the higher request set. Here they additionally give the adaptability to locate numerous base backings which is helpful for examination with related things and element bolster range. Their calculation gives the adaptability to enhanced affiliation and element support. Near result demonstrates the viability of their calculation.

In 2012, MiikaKomu *et al.* [34] recommend that distributed computing enhances usage and adaptability of assigning registering assets while lessening the infrastructural expenses. Be that as it may, cloud innovation is still restrictive much of the time and is polluted by security issues established in the multi-inhabitant environment of the cloud. For example, the virtual machines of two contending organizations could be served by the same fundamental host machine in an Infrastructure as a Service (IaaS) sort of cloud and this speaks to a security risk to be tended to. As an answer for this multi-occupancy issue, the Host Identity Protocol (HIP) offers an institutionalized approach to validate and ensure information streams between inhabitants fitting in with the same security area. Their tried different things with HIP keeping in mind the end goal to address the multi-inhabitant difficulties for open and cross breed IaaS mists. In their configuration, engineers and managers can get to cloud benefits straightforwardly over HIP, though purchasers get to the cloud without HIP utilizing an opposite HTTP intermediary. The intermediary likewise goes about as a heap balancer for a conveyed test administration sent both in an EC2 open cloud and a private cloud. The execution of the framework offers productivity equivalent to SSL and basically uses the same cryptographic calculations with comparable handling expenses. Thus, this infers that their proposed plan is a suitable distinct option for alleviate a percentage of the protection issues identified with multi-occupancy inside of a solitary server farm and to secure correspondences between two mists on account of a cross breed cloud.

In 2012, NicoR'odderet *al.*[35] distinguishes the need to look past specialized issues and turns the regard for enhancing agreeability and administration in cloud situations. In this procedure the attention is situated on the

irregularity top between existing techniques to recognize and assess IT hazards and the treatment of these dangers with Service Level Agreements. To close this top a model for a dynamic view on current IT hazard is proposed to consent to cutting edge IT situations that are made out of an abundance of distinctive administrations. The model has an in number corporate setting and will help organizations to assess their present danger introduction and in this manner, settle on better choices when picking their administrations.

In 2013, SreekumarVobugariet *al.* [36] propose that distributed computing has brought the spotlight as for the present business situation because of its multi-occupant and pay-as-you-utilize models, where clients require not make a big deal about purchasing assets like equipment, programming, foundation, and so forth on a for all time premise. As much as the innovative advantages, distributed computing likewise has its drawback. By taking a gander at its money related advantages, clients who can't manage the cost of beginning ventures, pick cloud by bargaining on its worries, similar to security, execution, estimation, accessibility, and so on. In the meantime, because of its dangers, clients – moderately larger part in number, evade relocation towards cloud. Considering this, execution and estimation are being the major basic components for any application sending in cloud environment. They give the guide to an enhanced execution driven distributed storage estimation approach, which is in light of adjusted PCTFree designation procedure for database frameworks arrangement in cloud environment. Goal of this methodology is to highlight the situated of key exercises that must be mutually done by the database specialized group and business clients of the product framework to perform an exact investigation to touch base at estimation for measuring of the database. For the assessment of this approach, a trial has been performed through differed size PCTFree portions on a trial setup with 100000 information records. The consequence of this examination demonstrates the effect of PCTFree arrangement on database execution. Premise this; they propose an enhanced execution driven distributed storage estimation approach in cloud.

In 2013, AzzedineBenameur *et al.* [37] present a way to deal with influence the flexibility and on-interest provisioning elements of the cloud to enhance strength to accessibility concerns and normal assaults. Their methodology uses expansion of lightweight virtualized application servers for repetition and security against both application lapses and system based attacks.

In 2013, Nikhilesh Pant *et al.* [38] presented the cloud reception and security framework. Their methodology suggested the intermediate aspects for data security and data aggregation.

In 2013, Du meng *et al.* [39] discussed about computing in the direction of security issues. They have applied admin side security as well as the data generalization approach has been included.

In 2013, Fan Yang *et al.* [40] suggested that the security issue is an important aspect in cloud computing. They have applied trusted cloud computing platform (TCCP). Trusted Coordinator (TC) has been adopted for different applications and security levels by the authors.

In 2014, Zhao *et al.* [41] recommend that the fast improvement of Cloud figuring is thwarted by numerous Cloud security issue. Distributed computing has numerous

qualities, e.g. multi-client, virtualization, adaptability etc. In light of these new attributes, conventional security advances can't make Cloud figuring completely safe. Thusly, Cloud figuring security turns into the ebb and flow exploration center. To take care of the issue of information security in distributed computing framework, by presenting completely homomorphism encryption calculation in the distributed computing information security, another sort of information security answer for the frailty of the distributed computing is proposed and the situations of this application is henceforth built. This new security arrangement is completely fit for the preparing and recovery of the scrambled information, and successfully prompting the expansive pertinent prospect, the security of information transmission and the stockpiling of the distributed computing.

3. PROBLEM IDENTIFICATION

After studying and analyzing several research papers in this field, we find some major security concerns which are following:

- Cloud processing is being embraced at a quick rate in light of the fact that it has a substantial number of upsides for a wide range of organizations and expands proficiency. Enterprises are decreasing cost expenses by utilizing online stockpiling arrangement suppliers. This permits the undertaking to store monstrous measures of information on outsider servers.
- One of the significant points of interest is that the massive amount storage limit is adaptable and accordingly, the undertaking pays for the measure of capacity that it needs. Moreover, access to the information is accessible through any Internet association. Adaptability and assignment of assets are the significant favorable circumstances of virtualization.
- Virtualization permits administrators to utilize handling power all the more proficiently and offer assets crosswise over equipment gadgets by overhauling multi-inhabitant clients. Chairmen can raise virtual machines (VMs) and servers rapidly without having the overhead of requesting or provisioning new equipment. Equipment assets that are no more needed for an administration or application can be re-doled out rapidly and additional handling force can be devoured by different administrations for greatest productivity.
- Though the presentation of distributed computing is in no way, shape or form the first innovation movement to bring about real security concerns, it is a huge development. As of not long ago, most associations have put away and dealt with their most discriminating data resources in physically isolated server farms either all alone premises or inside leased facilitating suppliers. So information centric security is required.
- Minimizing the information security dangers, while moving and putting away information, was simpler for associations to control inside of private server farms than inside of the cloud. Putting away information in

the cloud implies that information will be intermixed on shared servers. In the event that organizations jump into cloud without considering the unintended results, basic corporate information like client data and licensed innovation are at expanded.

- One of the most concerning drawbacks is the potential loss of control over some or the majority of the cloud environment that houses the information. Distributed computing is regularly isolated into three primary administration sorts: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and every effects information control and administration a little in an unexpected way. With IaaS, the client may have full control of the genuine server setup conceding them more hazard administration control over the earth and information. In PaaS, the supplier deals with the equipment and hidden working framework which confines endeavor hazard administration abilities on those segments. With SaaS, both the stage and the framework are completely overseen by the cloud supplier which implies if the fundamental working framework or administration isn't designed legitimately the information in the higher layer application may be at danger.
- If information isn't appropriately secured, misfortune and presentation can happen in the cloud whether it's a private on-reason cloud or an open one.
- Due to element adaptability, administration deliberation, and area straightforwardness components of distributed computing models, a wide range of utilizations and information on the cloud stage have no altered framework and security limits. In the occasion of security break, it's hard to segregate a specific physical asset that has a danger or has been compromised.
- As the openness of cloud and sharing virtualized assets by multi-inhabitant, client information may be gotten to by other unapproved sources.

4. DISCUSSION AND ANALYSIS

According to the Open Security Foundation, the individuals who keep up the most complete and helpful database of information break episodes, are currently likewise keeping up a database of distributed computing occurrences. This is accessible at cloutage.org. The data shown in figure 1 is taken from this.

There are as of now 213 episodes in this information base. Of these, 128 are named outages, 40 are named auto fails, 37 are named vulnerabilities, 4 are named instances of data loss and 4 are delegated hacks. Here's what that looks like when you chart it. Obviously, blackouts are still the most widely recognized issue, in spite of the fact that they likely don't bring about clients of distributed computing the same migraines that having touchy information traded off does. Security levels and assumption points as shown in figure 2. For figure 2 the base is taken as 1. Data sharing breaches and possible security threats can be better understood by figure 3.

Table 1: Result Analysis

S.no	Authors	Year	Work	Gap
1	Joshi et al. [42]	2012	They mainly concentrate on six different security majors which are Confidentiality, Availability, Integrity, Possession, Authenticity and Utility. They implement these phenomena in java.	Hybridization is missing.
2	Liu et al. [43]	2013	Security problems have been discussed	How the issues are resolved is missing.
3	Benameur et al. [44]	2013	How to handle the common attacks.	How it is implemented on different file system.
4	Li et al. [45]	2014	Weight sample can be used for data categorization.	Other clustering parameters can be added.
5	Yang et al. [46]	2013	They have applied elliptic curve diffie-hellman(ECDH).	Multi-layer security is missing.
6	Wang et al. [47]	2013	They introduced a third party auditor (TPA) for the basis of cloud client and supports dynamic data storage.	More enhancement is needed.
7	Sampada et al. [48][49]	2013	They apply Chi-Square test, to test the hypothesis for correctness. The program capability was based on three parameters; first is F-measure (FM), second is odds ratio (OR) and third is power (PO).	Only software metrics are checked
8	Sivanandan et al. [50]	2015	Agile Methodology can be used for Code Quality, Code Bisector and Dynamic Regression checking.	Security measures are not defined.
9	Padhy et al. [51]	2011	Analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises.	Practical implementation is left.

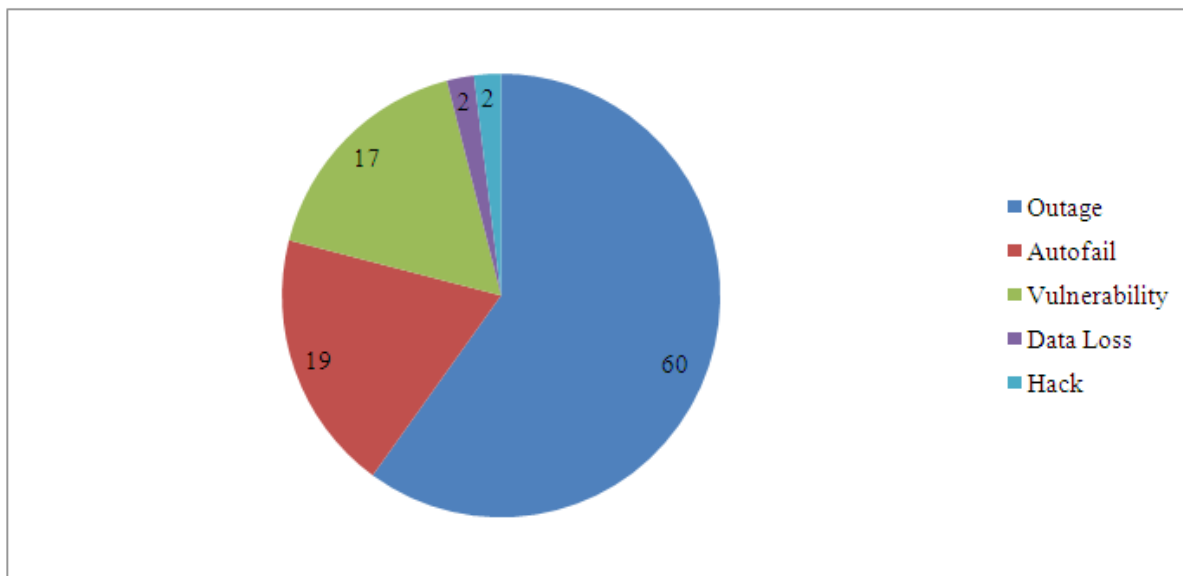


Figure 1: Security Distribution [Open Security Foundation]

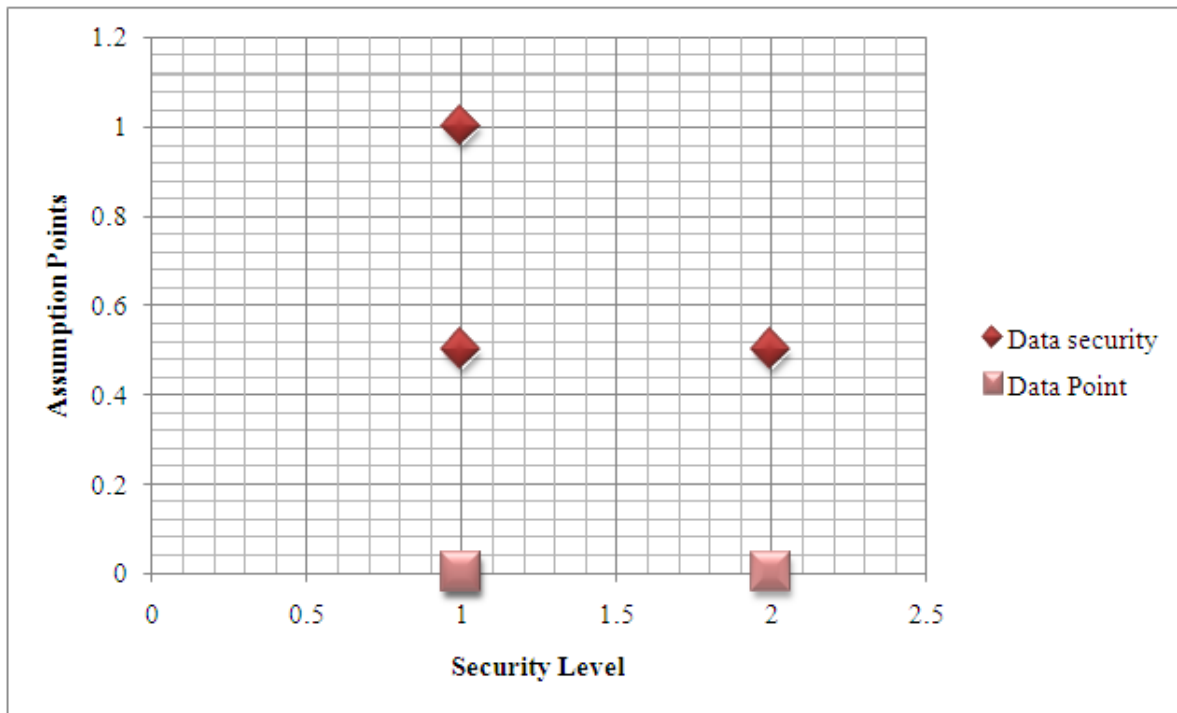


Figure 2: Security Levels

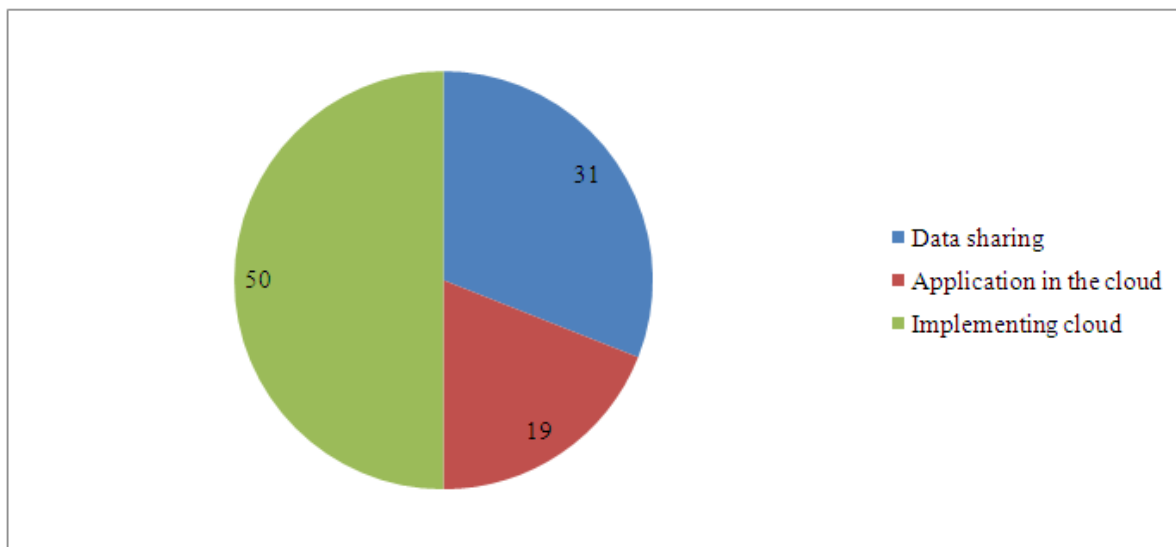


Figure 3: Chances of data attacks

5. CONCLUSIONS AND FUTURE DIRECTIONS

Data security in prospect of cloud computing is the major research area now a day as the cloud users are increasing day by day. In this paper we have reviewed and analyzed several previous researches works and suggest data centric approach to secure the data in the cloud computing environment. So, our paper guideline mean is to think about and investigates the benefits and discovering the crevice.

The future suggestions are following:

- Security is needed in all abstraction levels.
- Need to apply the security standards along with the technology collaborations to enhance the aggregation.
- To ease the deployment and development.
- The client cedes control to the Provider on a number of issues effecting security and provide proper justification on the below points:
 Very limited logs available.
 Usually no forensics service offered.
 No information on third-parties.
- Cloud Provider does not permit audit by the Cloud Customer. But we are planning it to be audited by the cloud auditor with some restriction.

- Key management and key provisioning can be allowed at the end of the cloud customers.
- Return on security investments (ROSI) the measures cloud computing can enable to improve the accuracy of ROI for security.
- Techniques for increasing transparency while maintaining appropriate levels of security: Tagging, e.g., location tagging, data type tagging, policy tagging.
- Privacy preserving data provenance systems, e.g., tracing data end-to-end through systems.

REFERENCES

- [1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
- [2] Igor Ruiz-Agundez, Yoseba K. Penya and Pablo G. Bringas, "Cloud Computing Services Accounting", International Journal of Advanced Computer Research (IJACR) ,Volume 2, Number 2, June 2012.
- [3] Ajey Singh, ManeeshShrivastava, "Overview of Security issues in Cloud Computing", International Journal of Advanced Computer Research (IJACR) Volume 2,Number 1, March 2012.
- [4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.
- [5] Ashutosh Kumar Dubey, Animesh Kumar Dubey, MayankNamdev, Shiv Shakti Shrivastava," Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG-2012.
- [6] A. Juels and B.S. Kaliski Jr., "Pors: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007.
- [7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.
- [8] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Report 2008/175, Cryptology ePrint Archive, 2008.
- [9] M. Naor and G.N. Rothblum, "The Complexity of Online Memory Checking," Proc. 46th Ann. IEEE Symp. Foundations of Computer Science (FOCS '05), pp. 573-584, 2005.
- [10] Wei-Tek Tsai, Xin Sun, JanakaBalasooriya , "Service-Oriented Cloud Computing Architecture" , 2010 Seventh International Conference on Information Technology.
- [11] G K Patra, NilotpalChakraborty," Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques", International Journal of Advanced Computer Research (IJACR) ,Volume-4 Number-1 Issue-14 March-2014.
- [12] NileshPachorkar, Rajesh Ingle," Multi-dimensional Affinity Aware VM Placement Algorithm in Cloud Computing", International Journal of Advanced Computer Research (IJACR) Volume-3 Number-4 Issue-13 December-2013.
- [13] <http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf>
- [14] SirwanGeramiparvar and Nasser Modiri, " Security as a Serious Challenge for E-Banking: a Review of Emmental Malware ", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-18, March-2015, pp.62-67.
- [15] Anita Venaik, "Qualitative risk level estimation of Business Process Re-engineering efforts and effects (With special reference to IT-sector)", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-18, March-2015, pp.11-18.
- [16] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609.
- [17] Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.
- [18] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of ASIACRYPT'08. Melbourne, Australia: Springer-Verlag, 2008, pp. 90–107.
- [19] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," Cryptology ePrint Archive, Report 2008/175, 2008.
- [20] M. Naor and G. N. Rothblum, "The complexity of online memory checking," in Proc. of FOCS'05, Pittsburgh, PA, USA, 2005, pp. 573–584.
- [21] E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.
- [22] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
- [23] Bhardwaj A, Subramanyam GV, Avasthi V, Sastry H. Review of solutions for securing end user data over cloud applications. International Journal of Advanced Computer Research. 2016 Nov 1;6(27):222.
- [24] Manimaran A, Durairaj M. The conjectural framework for detecting DDoS attack using enhanced entropy based threshold technique (EEB-TT) in cloud environment. International Journal of Advanced Computer Research. 2016 Nov 1;6(27):230.
- [25] Shobha K, Nickolas S. Time domain attribute based encryption for big data access control in cloud environment. ACCENTS Transactions on Information Security. 2017; 2(7):73-77.
- [26] NaikMR, Sathyanarayana SV. Key management infrastructure in cloud computing environment-a survey. ACCENTS Transactions on Information Security. 2017; 2(7):52-61.
- [27] Alotaibi MB. Antecedents of software-as-a-service (SaaS) adoption: a structural equation model. International Journal of Advanced Computer Research. 2016 Jul 1;6(25):114.
- [28] Tiwari R, Sinhal A. Block based text data partition with RC4 encryption for text data security. International Journal of Advanced Computer Research. 2016 May 1;6(24):107.
- [29] Fan Z, Wu Q, Zhang M, Zheng R. Popularity and gain based caching scheme for information-centric networks. International Journal of Advanced Computer Research. 2017 May 1;7(30):71.
- [30] Soni A, Hasan M. Pricing schemes in cloud computing: a review. International Journal of Advanced Computer Research. 2017 Mar 1;7(29):60.
- [31] Muthunagai, S. U.; Karthic, C. D.; Sujatha, S., "Efficient access of Cloud Resources through virtualization techniques," Recent Trends In Information Technology (ICRTIT), 2012 International Conference on , vol., no., pp.174,178, 19-21 April 2012.
- [32] AlZain, M.A.; Soh, B.; Pardede, E., "A New approach using redundancy technique to improve security in cloud computing," Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on , vol., no., pp.230,235, 26-28 June 2012.
- [33] Yun Yang; Lie Wu; Shasha Yang, "The Structure of Intelligent Grid Based on Cloud Computing and Risk Analysis," Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2012 4th International Conference on , vol.2, no., pp.123,126, 26-27 Aug. 2012.
- [34] Komu, M.; Sethi, M.; Mallavarapu, R.; Oirola, H.; Khan, R.; Tarkoma, S., "Secure Networking for Virtual Machines in the Cloud," Cluster Computing Workshops (CLUSTER

- WORKSHOPS), 2012 IEEE International Conference on , vol., no., pp.88,96, 24-28 Sept. 2012.
- [35] Rodder, N.; Knapper, R.; Martin, J., "Risk in modern IT service landscapes: Towards a dynamic model," Service-Oriented Computing and Applications (SOCA), 2012 5th IEEE International Conference on , vol., no., pp.1,4, 17-19 Dec. 2012.
- [36] Vobugari, S.; Somayajulu, D.V.L.N.; Subraya, B.M.; Srinivasan, M.K., "A Roadmap on Improved Performance-centric Cloud Storage Estimation Approach for Database System Deployment in Cloud Environment," Mobile Data Management (MDM), 2013 IEEE 14th International Conference on , vol.2, no., pp.182,187, 3-6 June 2013.
- [37] Benameur, A.; Evans, N.S.; Elder, M.C., "Cloud resiliency and security via diversified replica execution and monitoring," Resilient Control Systems (ISRCs), 2013 6th International Symposium on , vol., no., pp.150,155, 13-15 Aug. 2013.
- [38] Pant, N.; Parappa, S., "Seeding the cloud in a secured way: Cloud adoption and security compliance assessment methodologies," Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on , vol., no., pp.305, 308, 23-25 May 2013.
- [39] Du meng," Data security in cloud computing", The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka.
- [40] Fan Yang; Li Pan; MuzhouXiong; Shanyu Tang, "Establishment of Security Levels in Trusted Cloud Computing Platforms," Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCoM), IEEE International Conference on and IEEE Cyber, Physical and Social Computing , vol., no., pp.2119,2122, 20-23 Aug. 2013.
- [41] Feng Zhao; Chao Li; Chun Feng Liu, "A cloud computing security solution based on fully homomorphic encryption," Advanced Communication Technology (ICACT), 2014 16th International Conference on , pp.485,488, 16-19 Feb. 2014.
- [42] Shikha Joshi, Pallavi Jain, " A Secure Data Sharing and Communication with Multiple Cloud Environments with Java API " , International Journal of Advanced Computer Research (IJACR), Volume-2, Issue-4, June-2012 ,pp.135-143.
- [43] Xiao-hui, Liu, and Song Xin-fang. "Analysis on cloud computing and its security." In Computer Science & Education (ICCSE), 2013 8th International Conference on , pp. 839-842. IEEE, 2013.
- [44] Benameur, Azzedine, Nathan S. Evans, and Matthew C. Elder. "Cloud resiliency and security via diversified replica execution and monitoring." In Resilient Control Systems (ISRCs), 2013 6th International Symposium on , pp. 150-155. IEEE, 2013.
- [45] Kai Li, Lijuan Cui, "A Kernel Fuzzy Clustering Algorithm with Generalized Entropy Based on Weighted Sample", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.596-600.
- [46] Yang, Ching-Nung, and Jia-Bin Lai. "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing." In Biometrics and Security Technologies (ISBAST), 2013 International Symposium on , pp. 259-266. IEEE, 2013.
- [47] Wang, Qian, Cong Wang, KuiRen, Wenjing Lou, and Jin Li. "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22, no. 5 (2011): 847-859.
- [48] SampadaKembhavi, Ravindra Gupta, Gajendra Singh, " An Efficient Algorithm for Auto Upload and Chi-Square Test on Application Software " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-10, June-2013 ,pp.121-125.
- [49] SampadaKembhavi and Gajendra Singh, " Auto Upload and Chi-Square Test on Application Software as a Service for Cloud Computing Environment " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 ,pp.26-31.
- [50] SandeepSivanandan, " Fail Fast - Fail Often: Enhancing Agile Methodology using Dynamic Regression, Code Bisector and Code Quality in Continuous Integration (CI) " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015 ,pp.220-224.
- [51] Padhy, Rabi Prasad, ManasRanjanPatra, and Suresh Chandra Satapathy. "Cloud computing: security issues and research challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1.2 (2011): 136-146.