Secure Data Storage and Retrieval in the Cloud

K. Ravindranath, M.S. Sandeep Reddy, M. Deepak Reddy, D. Chaitanya

Abstract: ***In Cloud client can remotely store and bring their information depending on their work need or interest, and cloud is very cheap and dependable too. But cloud has major problem regards to its security, it solely depends upon the cloud provider. In this paper we deal with providing security to the information. In proposed technique it provides a secured way to upload the information by encrypting it before being uploaded to cloud and decrypting with verified secret key before downloading***

Keywords: Cloud Computing, Cloud security, privacy preserving

I. INTRODUCTION

Cloud specialist co-ops are planned to give various capacity services[10]. Clients will be profited as they can store substantial measure of information in outsider stockpiling sparing their very own framework space. The most essential and noticeable issue to be tended to is security. Cloud server providers offer different security components, however in the event that an enemy gains admittance to the client's information, at that point it influences the protection of the client. Security ought to be accommodated touchy information of the client through different authentication and approval components. For the most part client information are verified by encryption and unscrambling techniques [5][13].

Information can be scrambled by changing over plain content into a figure content utilizing the sender's open key and unscrambled by changing over figure content into plain content by the private key. Different cryptographic calculations.

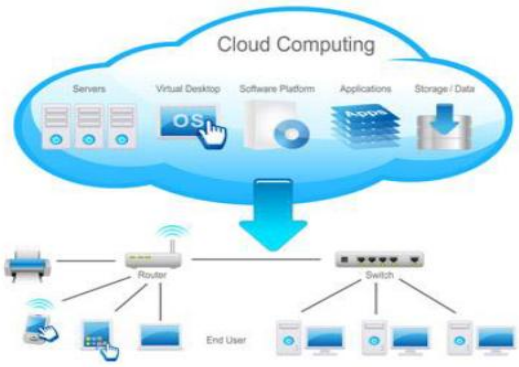

Fig. 1 Cloud service architecture

Revised Manuscript Received on April 12, 2019.

K. Ravindranath, Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

M.S. Sandeep Reddy, B.Tech Student, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

M. Deepak Reddy, B.Tech Student, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

D. Chaitanya, B.Tech Student, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

Cloud computing is an exude worldview custom-made to meet business and research needs. The cloud storage offers different focal points, for example, substantial measure of storage in the Pay-Per-Use arrangement, information accessibility, and quick access for the recovery of information [14]. Cloud computing layers are in charge of various kinds of administrations we obtain. SaaS layer gives access to different programming which can be utilized according to our need as opposed to downloading and introducing in the framework. Iaas oversees virtual machines, systems and so forth.

PaaS gives office passage utilizing various applications or administrations by decreasing the staggering expense and trouble of purchasing and overseeing the essential abilities of present programming and equipment.

Cloud Database

In cloud computing pay as u go is current trend. It implies clients simply need to pay just for the administrations utilized. These days cloud database administrations are rising as a standout amongst the most imperative administrations among cloud computing [13].

At the point when expansive separation must be secured and information must be exchanged per terabyte, it costs much. That is the reason cloud database turned out to be prevalent as it gives various focal points. Cloud Database gives low and modest cost accessibility to clients. On account of cloud computing trademark highlights, for new applications cloud computing gives best and efficient approach to set up and help numerous little scale business to come up which were already not ready to come up because of money related issue in old customary technique.

The present-day accomplishments in information, versatile, remote and Internet advancements can't be amplified. Also, thus Cloud processing is a rising business show that guarantees to kill the requirement for keeping up costly figuring offices by organizations and establishments alike. Cloud computing innovation influences it conceivable to create and have an application structure for the web where data innovation (IT) related offices are given "as an administration"; enabling customers to get to innovation empowered administrations all the more financially and adaptability on a pay-as-you-use premise[7].

Cloud computing applications are cloud based administrations otherwise called Software as a Service (SaaS). These cloud applications can do anything ranging from monitoring notes and to bookkeeping. Cloud based application also provide their users access to their data from any place in the world.

This provides cooperation, to access their data from any were with any delay after uploading into cloud.

Cloud Database as a Service

Database Management System is an application which gives the creation, the executives of the database. Experts can enter new records, refresh, alter and erase information at whatever point required [12]. Clients can deal with all undertakings identified with information, likewise addition and change. Reports, question, and tables are for the most part portions of database taking care of programming called database the executives programming.

The idea of cloud computing in time long past occasions was being made out of five attributes, four organization models and three administration models however in the present situation, it is being expanded and more classifications have been included like Storage-as-a-Service, Security-as-a-Service and Database-as-a-Service. As of late, an imperative piece of the cloud is an adaptable database which includes refreshing of work and choice framework.

The manner in which the information was being spared and recovered is being changed with the rise of cloud database. Given a cost value, servers and applications like database are given as cloud administrations[1][17].

In evolving pattern, numerous specialized preferences like no compelling reason to burn through cash in physical setup of database workplaces and dealing with undertakings since assets are accessible as administrations online.Figure.3 depicts the dimensions of cloud engineering in which a client can store the information safely and it very well may be recovered securely. Presently the prerequisite of having server farms is done as cloud database give administration effectively. Clients may likewise make possess applications which are conceivable in view of assets being given by PaaS model to cloud databases.

II. LITERATURE REVIEW

D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III assume the issue; were alex wishes to keep the email using providers like lexa (like gmail and so on) now lexa has to provide alex with the capacity gather and gets messages and also the provider in the mean time check number of messages sent to deepak with harsha as the middle man. At first the messages is sent to harsha in encoded structure and alex at any point of time ask lexa to send duplicate of entire database in scrambled messages. This is not efficient. Int his paper we give the best way to open key encryption plots for alex that will provide the pir seeking the encoded records.the solution is that it should not have any halfway data regards to user enquiry. The principle procedure of solution also will take single database api into account.

O. Goldreichand R. Ostrovsky, software protection is crucel in pc use. There are several number of strategies and heuristics for this. In this paper we discuss the hypothetical treatment of programming assurance. In this we provide the programming insurance proficient use of RAM. A machine is careless if the gathering in which it gets to memory zones is relative for any two commitments with a comparable running time. For example, an ignorant Turing Machine is one for which the advancement of the heads on the tapes is undefined for each computation. (Along these lines, it is free of the certifiable data.) What is the log jam in the running time of any machine, in case it is required to be missing?

In 1979 Pippenger and Fischer showed how a two-tape careless Turing Machine can reenact, on-line, a one-tape Turing Machine, with a logarithmic stoppage in the running time. We show a like outcome for the sporadic access machine (RAM) model of estimation. In particular, we advise the most ideal approach to finish an on-line diversion of an optional RAM commitment by a probabilistic careless RAM with a poly-logarithmic stoppage in the running time. On the other hand, we exhibit that a logarithmic stoppage is a lower bound.

Q. Liu, G. Wang, and J. Wu, The users stores their data in cloud and excess them from anywhere when they need the data. The user should upload his data in a encrypted form and later after the upload send question as encoded watchwords. Here the basic encryption form may not be efficient when the user wants to download a certain type of document use some catchphrases. To begin with the user needs to scramble decode the document as regular as possible which cpu intense and following to that we cannot determine which files contain the keywords. So it just returns all the encrypted files. So this not practical considering the present situation. In this paper, we inquire about the characteristics of cloud computing, and, propose, an efficient insurance shielding keyword, search scheme, in distributed computing. It allows an organization provider,to check out deficient decipherment, to decline a client's computational overhead, and engages the organization provider, to glance through the keywords, on encrypted, files to guarantee the customer data privacy, and, the customer request privacy, efficiently. By affirmation, our arrangement is semantically secure.

III. REQUIREMENTS OF CLOUD DATABASE MANAGEMENT IN CLOUD

Regardless of whether an association has been taken, an examination focus, or any instruction focus it remains the essential needs to process information quick and in a productive way. For this reason, organizations plan and oversee database preparing undertakings in order to deal with work of database, for example, introducing, looking after tasks[6]. Database related monotonous assignments are particularly hard to oversee and a little issue forgot will turn confounded , instead of purchasing equipment and items identified with database ,associating the systems alongside utilizing experienced people it will be smarter to make utilization of cloud database administrations on account of reasonableness and simpler and successful administration of database related errands .

Budgetary venture tends not to change as various equipment, programming and systems expenses may diminish yet expenses of individuals overseeing such confounded undertakings keep on expanding[1]. It might happen that experts costs will rule over the answer for database dealing with expenses. For having a course of action of information, the database should be rebuilt,

cosmetics with certain changes, reestablished, take a reinforcement, to make alterations for dividing. There isn't much advancement in the territory when there no effect on the availability of database arrangement, and still development from one database to next winds up conceivable. Since climbing from one database to next makes a few parts inaccessible to utilize[13].

Areas where PCs and related parts are being housed or server farms all the more decisively, are utilizing database the executives frameworks. Be that as it may, a lot prior it was dependent upon the designers to choose the kind of database for the cloud and play out the introducing and overseeing undertakings. They additionally need to manage the entangled organization assignments all alone. Positive viewpoints are full control is given as a determination of claim database and its managing should be possible.

PaaS Service merchants presently furnish up with database benefits on a cloud so as to diminish the outstanding burden of cloud clients and the work is taken over by cloud supplier who deals with controlling everything beginning from the treatment of logs to recuperating and support up all things considered. The designer needs to bargain up to table and question support. In some cases there is an association which takes up errands of database administrations [9].

For the creation, stockpiling and the executives of database undertakings there are numerous database specialist co-ops. As opposed to utilizing association registering framework, clients can get to information utilizing equipment and programming by the specialist organization. Presently positive viewpoints are many, similar to it might happen that at database specialist organizations side there might be a changing in programming, equipment or systems administration side or there might be a disappointment however the clients will have no impact on the issue since it will be managed database specialist co-ops side[3][10].

For the most part, the association just takes into utilization framework for database benefits whose organization is finished by specialist co-ops. Presently there is no requirement for purchasing, altering, refreshing and performing such assignments identified with the database by cloud clients.

Regardless of whether it is budgetary, business, or any web related work, database is required wherever for a few or the other reason. The old strategy, which is known as a conventional database system[8] which was much being used. A few impediments of this database frameworks are –

1) Difficult support works
2) Scalability and setup issues
3) Complication in browsing the accessible frameworks
4) cost of certain frameworks substantially more than anticipated

So these weaknesses are handled up by the cloud-based Database as an administration. In the present situation, any DBaaS highlights can't discover that can adapt up to every one of the weaknesses. So there will be next blast of an advancement of database.

IV. DATA SHARING SCHEMES

Cloud computing [1] is playing a crucial role in development in storing of data, processing and distribution. But storing of data in cloud has both advantages and disadvantages. The advantage is that it provides the means for easy data sharing and reduces the necessity for local storage of data at much less cost. The disadvantage is regards to security of data that is deployed in cloud. As the data deployed in cloud is stored remotely somewhere around the world. The solution for this is encrypting the data before upload it on to cloud [13].

System Model

This consists of the following entities group manager, cloud, group member as shown in below figure 2

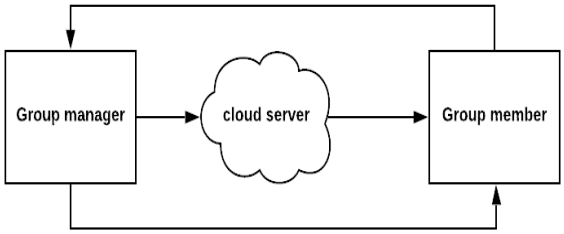

Fig. 2 Data Sharing Model

Cloud: cloud is where we store our data and is operated by cloud service provider

Group Manager: The group manager acts as a administrator of the group. Group manager manages the new user registrations and revocation of user. And revealing the real identity of the owner in any case of dispute. Group manager is the person who is fully trusted by all group members

Group Members: Group members are registered users. Group members can store their data in cloud and also share it between the members of the group

There are several security schemes for sharing data on malicious servers. On such that we saw is encrypting the data before being shared to cloud by the user and sharing the key to receipt of the data for decrypting by. By doing this the content of data is not leaked to unauthorized users [11]. Nonetheless, as the quantity of information proprietors and the quantity of repudiated clients increment, the complexities of client cooperation and disavowal in these plans are expanding linearly. MONA infers that any client in the gathering can safely impart information to others by the untrusted cloud.

Multi owner data sharing use the group signature and dynamic encryption. By using these users can share the data securely through untrusted cloud. Group signature will help the users to excess cloud anonymously. Broadcast encryption helps in sharing of information with the other users of group. In information sharing plans, to give information classification to dynamic broadcast encryption every client needs to process the revocation parameters which helps in keeping the information protected from the renounced users[13][10].

In any such cases, revocation results in computation overhead of encryption. The size of cipher text increase with increase in revoked users. As result large cipher text and heavy over head makes to take dynamic broadcast scheme.

This kind of disadvantage can be overcome by decreasing the computation overhead of users and cipher text, the group manager comes into play and compute the revocation parameters and transfer the same to cloud, here every one can see this results as it is pubic. This not only overcome the above problems but also makes them to be constant and also be independent of the number of revoked users.

V. EXPERIMENTS AND RESULTS

Home page

The preview underneath demonstrates the landing page of the proposed framework. The landing page is made utilizing html language. It has connections to client enrollment, client login and client transfer pages.

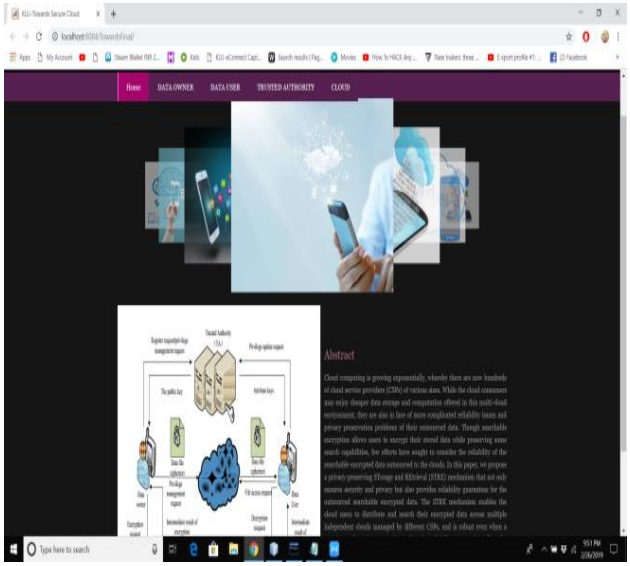

Fig. 3 Data Uploading Page

Encryption/Decryption

This page is made to demonstrate the scrambled and unscrambled estimation of document key. It would likewise show the records transferred to cloud server.

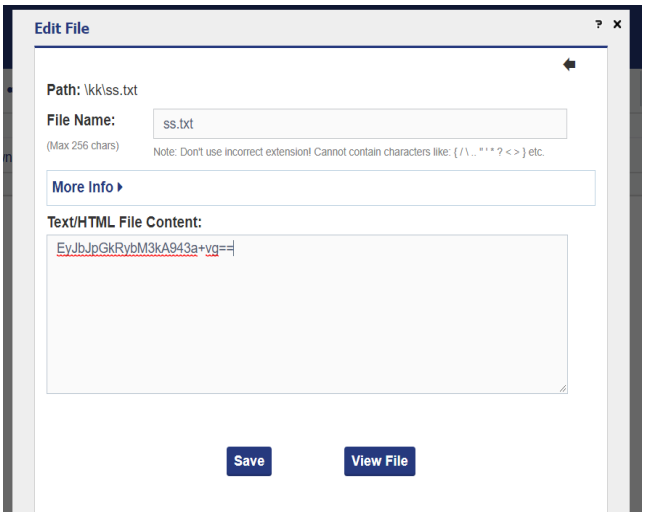

Fig. 4 Encryption/decryption

User Download Page

How the client can download from the server database. In this page the client will be given with alternatives for document, content or picture download.

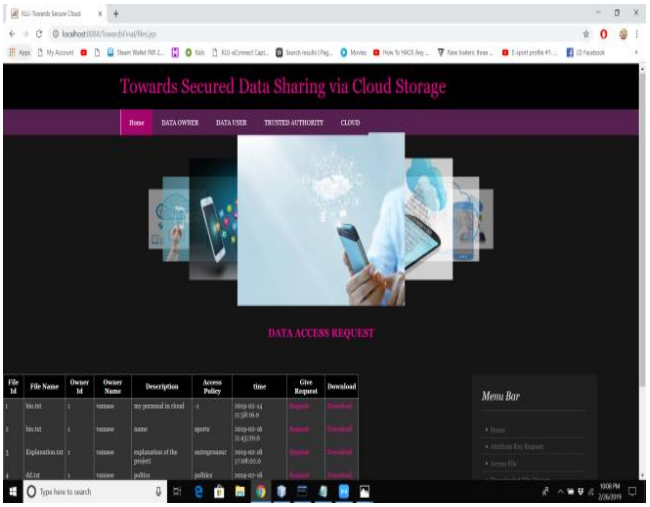

Fig. 5 user download page

VI. CONCLUSION

The proposed framework viably gives secure information transferring and recovery by utilizing AES and FHE. AES gives greater security to the framework as it isn't defenseless against any known jump. The proposed framework additionally expands the precision and accessibility of client information in the cloud. Proposed component gives such a useful system plan which accomplishes input/yield protection, tricking adaptability, and proficiency in the cloud.

VII. FUTURE WORK

The present venture can be reached out to following future enhancement.

The calculation can likewise be amplified to not just encode information i.e., record, picture and content yet additionally sound and video files.

REFERENCES

1. Bhabendu Kumar Mohanta, Debasis Gountia, “Fully homomorphic encryption equating to cloud security: An Approach”, IOSR Journal of Computer Engineering (IOSR- JCE), Vol 9, Jan-Feb 2013, PP 46-50, ISSN: 2278-8727.
2. B. Krebs, “Payment Processor Breach may be Largest Ever,” http://voices. washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, 2009.
3. G. Brunette, R. Mogull et al., “Security Guidance for Critical Areas of Focus in Cloud Computing v2. 1,”Cloud Security Alliance, pp. 1–76, 2009.
4. K. Ren, C. Wang, Q. Wang et al., “Security Challenges for the Public Cloud,” in IEEE Internet Computing,vol. 16, no. 1, pp. 69–73, 2012.
5. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure Ranked Keyword Search over Encrypted Cloud Data,” in Proceedings of the IEEE 30th International Conference on Cloud Computing Systems (ICDCS), pp.253–262, 2010.

6. A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the Clouds: A Berkeley View of Cloud Computing," Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, pp.1–23, 2009.
7. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, andI. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.
8. M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," Online at http://www. techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-emaildeletions, 2006.
9. A. S. Team, "Amazon S3 Availability Event: July 20, 2008,"http://status.aws.amazon.com/s3-20080720.html, 2008.
10. H. Perl, Y. Mohammed, M. Brenner, and M. Smith, "Privacy/Performance Trade-off in Private Search on Bio-Medical Data," Future Generation Computer Systems, vol. 36, pp. 441–452, 2014.
11. R Gennaro, C Gentry, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers", 30th annual conference on Advances in cryptology, Berlin, 2010, ISBN: 3-642-14622-8 978-3-642-14622-0.
12. Kan Yang, Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", International Conference on parallel and distributed systems, Vol 24, no 9, September 2013, ISSB : 1045-9219/13.
13. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, Hangzhou, 23-25 March 2012, PP 647-651, ISBN:978-1-4673-0689-8.
14. Z. Slocum, "Your Google Docs: Soon in Search Results? "http://www.cnet.com/news/your-google-docssoon-in-search-results/, 2009.
15. S Hohenberger, A Lysyanskaya, "How to securely outsource cryptographic computations", February 16, 2005, PP 1-19.
16. C Gentry, "Computing arbitrary functions of encrypted data", Magazine on Communications of the ACM, New York, Vol 53, March 2010, PP 97-105, DOI:10.1145/1666420.1666444.
17. Cloud Computing: Special theme, European research consortium for Informatics and mathematics (ERCIM), ISSN 0926-4981.
18. Charan, N.S., Kishore, K.H. Recognization of delay faults in cluster based FPGA using BIST (2016) Indian Journal of Science and Technology, 9 (28).
19. Hari Kishore, K., Aswin Kumar, C.V.R.N., Vijay Srinivas, T., Govardhan, G.V., Pavan Kumar, C.N., Venkatesh, R.V. Design and analysis of high efficient UART on spartan-6 and virtex-7 devices (2015) International Journal of Applied Engineering Research, 10 (9), pp. 23043-23052.
20. Kante, S., Kakarla, H.K., Yadlapati, A. Design and verification of AMBA AHB-lite protocol using Verilog HDL (2016) International Journal of Engineering and Technology, 8 (2), pp. 734-741.
21. Bandlamoodi, S., Hari Kishore, K. An FPGA implementation of phase-locked loop (PLL) with self-healing VCO (2015) International Journal of Applied Engineering Research, 10 (14), pp. 34137-34139.
22. Murali, A., Hari Kishore, K., Rama Krishna, C.P., Kumar, S., Trinadha Rao, A. Integrating the reconfigurable devices using slow-changing key technique to achieve high performance (2017) Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017, art. no. 7976849, pp. 530-534.
23. A. Surendar, K. H. Kishore, M. Kavitha, A. Z. Ibatova, V. Samavatian "Effects of Thermo-Mechanical Fatigue and Low Cycle Fatigue Interaction on Performance of Solder Joints" IEEE Transactions on Device and Materials Reliability, P-ISSN: 1530-4388, E-ISSN: 1558-2574, Vol No: 18, Issue No: 4, Page No: 606-612, December-2018.
24. N Bala Dastagiri K Hari Kishore "A 14-bit 10kS/s Power Efficient 65nm SAR ADC for Cardiac Implantable Medical Devices" International Journal of Engineering and Technology (UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 2.8, Page No: 34-39, March 2018.
25. N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.
26. N Bala Dastagiri, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.
27. Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.
28. Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks and Soft Computing,ISSN:978-1-4799-3486-7/14,pp.248-251,August 2014.
29. P Bala Gopal, K Hari Kishore, R.R Kalyan Venkatesh, P Harinath Mandalapu "An FPGA Implementation of On Chip UART Testing with BIST Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015.
30. Avinash Yadlapati, Hari Kishore Kakarla **"**Design and Verification of Asynchronous FIFO with Novel Architecture Using Verilog HDL**"** Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No: 14, Issue No: 1, Page No: 159-163, January 2019.
31. Yadlapati, A., Kakarla, H.K. An Advanced AXI Protocol Verification using Verilog HDL (2015) Wulfenia, 22 (4), pp. 307-314.
32. Bindu Bhargavi, K., Hari Kishore, K. Low Power Bist on Memory Interface Logic (2015) International Journal of Applied Engineering Research, 10 (8), pp. 21079-21090.