International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Result paper on Designing Multi-Cloud Server for Scalable and Secure Sharing over Web

[-1*] Shruti Timande,
[1] Department of Wireless Communication and Computing, RTMNU University, TGPCET Nagpur, Maharashtra, India
[2] Prof. Sulabha Patil
[2] Assistant Professor Computer Science and Engineering, RTMNU University, TGPCET Nagpur, Maharashtra, India

ABSTRACT
With the internet getting so popular data sharing and security of personal data has gain much more importance than before. Cloud provides and efficient way to outsource the data either online or offline but data security becomes one of the major issues in unreliable multi-cloud environment. This paper addresses the issues in multi-cloud environment and also provides a way to provide better security in multi-cloud environment. Further it discusses the different encryption algorithms that can be used to maintain a design framework for cloud environment.

KEYWORDS: Cloud Computin; IaaS; Encryption; SaaS; PaaS; Distributed; Security; Split; Merging; Encryption

INTRODUCTION

Engineering development and its selection are two discriminating effective variables for any business/association. Cloud computing is a late innovation ideal model that empowers associations or people to impart different administrations in a consistent and practical way. Cloud computing exhibits an opportunity for pervasive frameworks to power computational and stockpiling assets to achieve assignments that would not typically be conceivable on such asset obliged gadgets. Distributed computing can empower programming and base planners to construct lighter frameworks that last more and are more convenient and versatile. Regardless of the favorable circumstances distributed computing offers to the originators of pervasive frameworks, there are a few impediments and constraints of distributed computing that must be tended to.

BRIEF LITERATURE SURVEY:

There are numerous issues with current cloud and their architectures. Some of them are clients are regularly tied with one cloud supplier, registering segments are firmly coupled, absence of SLA backings, absence of Multi-tenure backings, Lack of Flexibility for User Interface. [4]

A standout amongst the most critical issues identified with cloud security dangers is information honesty. The information put away in the cloud may experience the ill effects of harm amid move operations from or to the distributed storage supplier. Cachinet al. give illustrations of the danger of assaults from both inside and outside the cloud supplier, for example, the as of late assaulted Red Hat Linux's conveyance servers. Another case of ruptured information happened in 2009 in Google Docs, which set off the Electronic Privacy Information Center for the Federal Trade Commission to open an examination concerning Google's Cloud Computing Services. Another illustration of a danger to information uprightness as of late happened in Amazon S3 where clients experienced information defilement.

One of the outcomes that they propose is to use a Byzantine imperfection tolerant replication tradition inside the cloud. Hendricks et al. express that this outcome can sidestep data debasement made by a couple parts in the cloud.

Of course, Cachinet al. affirm that using the Byzantine imperfection tolerant replication tradition inside the cloud is unsuitable on account of the way that the servers having a spot with cloud suppliers use the same structure foundations and are physically set in the same spot [1]. According to Garfinkel, another security danger that may happen with a cloud supplier, for instance, the Amazon cloud organization, is a hacked mystery key or data interference. If some individual becomes acquainted with an Amazon account mystery key, they will have the ability to get to most of the account's events and resources [1].

In spite of the way that cloud suppliers are aware of the pernicious insider danger, they expect that they have fundamental responses for mollify the issue [1]. Rocha and Correia [1] center possible aggressors for Iaas cloud suppliers. For representation, Grosse et al. [1] propose one result is to keep any physical access to the servers. Regardless, Rocha and Correia [1] fight that the aggressors depicted in their work have remote get to and needn't trouble with any physical access to the servers. Grosse et al. [1] propose a substitute result is to screen OK to get access to the servers in a cloud where the customer's data is secured. In any case, Rocha and Correia [1] state that this segment is beneficial for watching laborer's behavior to the extent whether they are after the insurance course of action of the association or not, on the other hand it is not fruitful in light of the way that it recognizes the issue after it has happened.

A substitute strategy to secure appropriated processing is for the data holder to store mixed data in the cloud, and issue unraveling keys to endorsed customers. By then, when a customer is revoked, the data administrator will issue re-encryption requests to the cloud to re-scramble the data, to keep the repudiated customer from unraveling the data, and to create new unscrambling keys to considerable customers, so they can continue getting to the data. Of course, since a circulated registering environment is included various cloud servers, such summons may not be gotten and executed by most of the cloud servers on account of hazardous framework correspondences [3].

A substitute way to deal with secure the data using various crushing and encryption estimations and to hide its range from the customers that stores and recoups it. The primary difference is that the system presented by Olfa Nasraoui [2] is an application based structure like which will keep running on the clients own structure. This application will allow customers to exchange record of different associations with security quirks including Encryption and Compression. The exchanged records may be gotten to from wherever using the application which is given.

The security of the Olfa Nasraoui [2] model has been examination on the reason of their encryption count and the key organization. It has been watched that the encryption estimation have their own specific properties; one figuring gives security to the detriment of fittings, other is strong however uses more number of keys, one takes moreover taking care of time. This territory exhibits the distinctive parameters which accept a foremost part while selecting the cryptographic computation. The Algorithm found most ensuring is AES Algorithm with 256 piece key size (256k) [2].

A standard trick of cloud is data advertising. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng [5] show to securely, viably, and adaptably give data to others in appropriated stockpiling. We depict new open key cryptosystems which convey relentless size figure messages such that capable task of unscrambling rights for any arrangement of figure works are possible. The interest is that one can add up to any arrangement of secret keys and make them as minimized as a singular key, yet wrapping the power of each and

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

every one of keys being gathered. Toward the day's end, the riddle key holder can release a reliable size aggregate key for versatile choices of figure substance set in appropriated stockpiling, however the other encoded records outside the set stay mystery [5].

There are diverse examination challenges in like manner there for grasping dispersed processing, for instance, for the most part managed organization level declaration (SLA), security, interoperability and steadfastness. This examination paper graphs what conveyed processing is, the diverse cloud models and the standard security threats and issues that are at present inside the dispersed figuring industry. This investigation paper moreover explores the key exploration and troubles that shows in appropriated registering and offers best practices to organization suppliers furthermore attempts wanting to power cloud organization to improve their final result in this genuine monetary environment [7].

Cloud based information stockpiling frameworks have numerous complexities with respect to basic/secret/touchy information of customer. The trust required on Cloud stockpiling is so far had been constrained by clients. The paper's part is to develop trust in Users towards Cloud based information stockpiling. The paper handles key inquiries of the User about how information is transferred on Cloud, kept up on cloud with the goal that there is no information misfortune; information is accessible to just approved User(s) according to Client/User prerequisite and propelled ideas like information recuperation on fiasco is connected [8].

PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner.

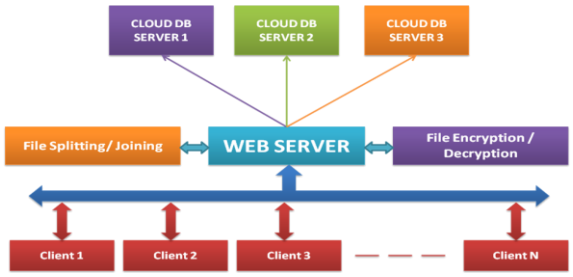
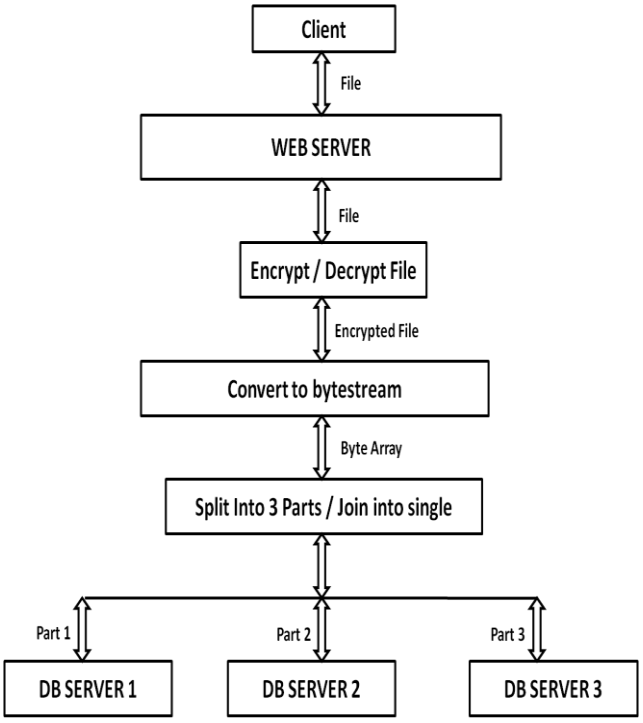


Fig: Basic Proposed System Architecture

The system will provide load balancing in terms of database as the file to be uploaded will be splitted into n parts and each part will be stored in a different cloud server. Consider an example where a file is splitted into two part out of which one is stored in google IaaS and other in Yahoo IaaS.
Below given is the basic flow diagram of the project. In above diagram whenever a client sends a file upload request, the web server takes the file encrypts it using AES algorithm then ZIP it and then splits the file into three equal parts and loads in three different database servers.



International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

AES algorithm

AES depends on an outline rule known as a Substitution stage system. It is quick in both programming and equipment. Not at all like its antecedent, DES, AES does not utilize a Feistel system. AES has a settled piece size of 128 bits and a key size of 128, 192, or 256 bits, though Rijndael can be indicated with square and key sizes in any different of 32 bits, with at least 128 bits.

The square size has a most extreme of 256 bits, however the key size has no hypothetical greatest. AES works on a 4×4 section significant request lattice of bytes, termed the state (renditions of Rijndael with a bigger piece size have extra segments in the state). Most AES counts are done in an extraordinary limited field.

Working Of AES:

Propelled Encryption Standard or AES was developed by Joan Daemen and Vincent Rijmen, and acknowledged by the US central government in 2001 for top mystery affirmed encryption calculations. It is likewise alluded to as Rijndael, as it is based off the Rijndael calculation. Supposedly, this standard has never been broken.

AES has three sanction key length: 128 bits, 192 bits, and 256 bits. To attempt to clarify the procedure in basic terms, a calculation begins with an arbitrary number, in which the key and information encoded with it are mixed however four rounds of numerical procedures. The key that is utilized to scramble the number must likewise be utilized to unscramble it.

The four rounds are called SubBytes, ShiftRows, MixColumns, and AddRoundKey. Amid SubBytes, a lookup table is utilized to figure out what every byte is supplanted with. The ShiftRows step has a sure number of lines where every line of the state is moved consistently by a specific counterbalance, while leaving the first column unaltered. Every byte of the second column is moved to one side, by a balance of one, every byte in the third line by a counterbalance of two, and the fourth line by a balance of three. This moving is connected to each of the three key lengths, however there is a change for the 256-piece square where the first column is unaltered, the second line balance by one, the third by three, and the fourth by four. The MixColumns step is a blending operation utilizing an invertible straight change as a part of request to join the four bytes in every section. The four bytes are taken as data and created as yield.

In the fourth round, the AddRoundKey gets round keys from Rijndael's key calendar, and adds the round key to every byte of the state. Every round key gets included by consolidating every byte of the state with the relating byte from the round key. Ultimately, these strides are rehashed again for a fifth round, however do exclude the MixColumns step.

These calculations basically take fundamental information and change it into a code known as figure content. The bigger the key, the more noteworthy number of potential examples that can be made. This makes it to a great degree hard to descramble the substance, which is the reason AES has been Teflon-covered

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

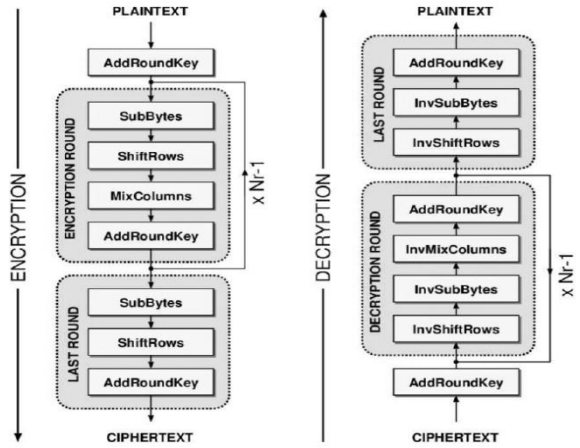


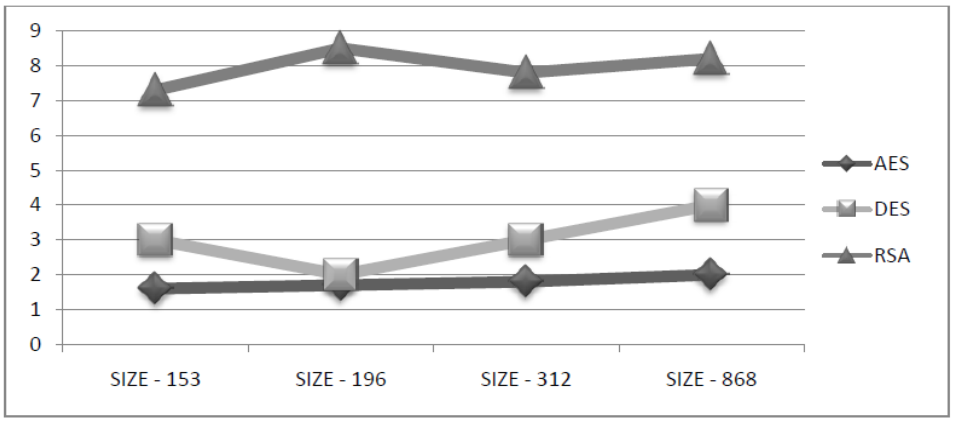
Fig: Working of AES algorithm

User Authentication

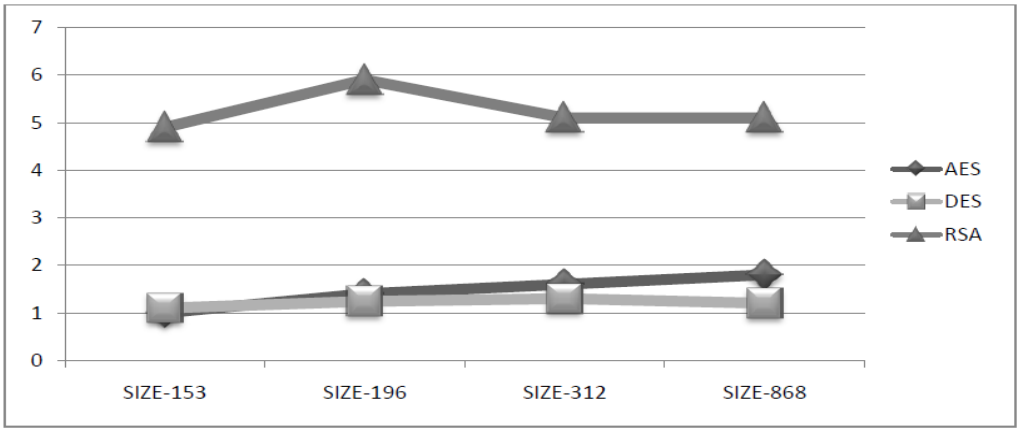
Basically whenever a user wants to use the system he/she is required to register onto the system if not registered. After registration the email is verified by sending the temporary password on mail itself. Ones the user has id and password he can login into the system and use system services.

RESULT ANALYSIS

Graph based Comparison of AES DES and RSA



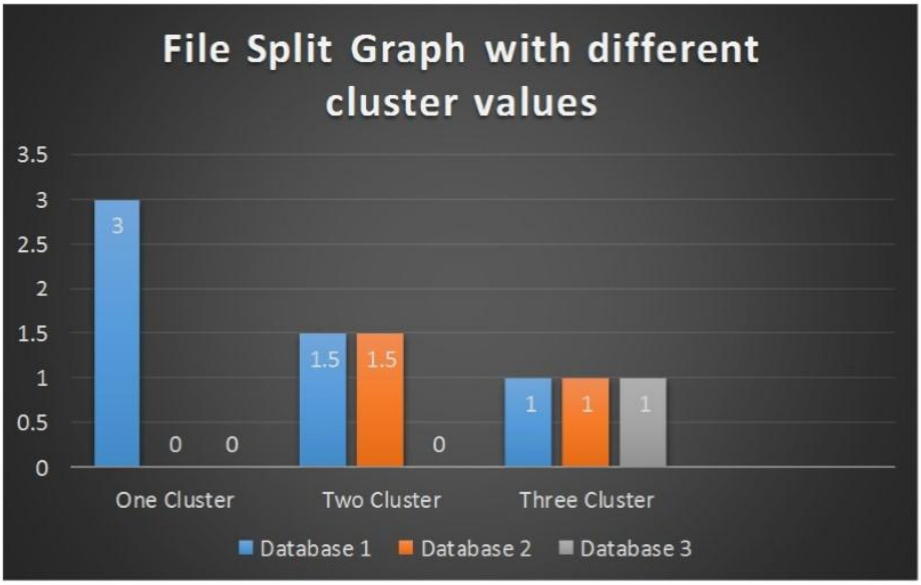
Encryption Time (in milliseconds)



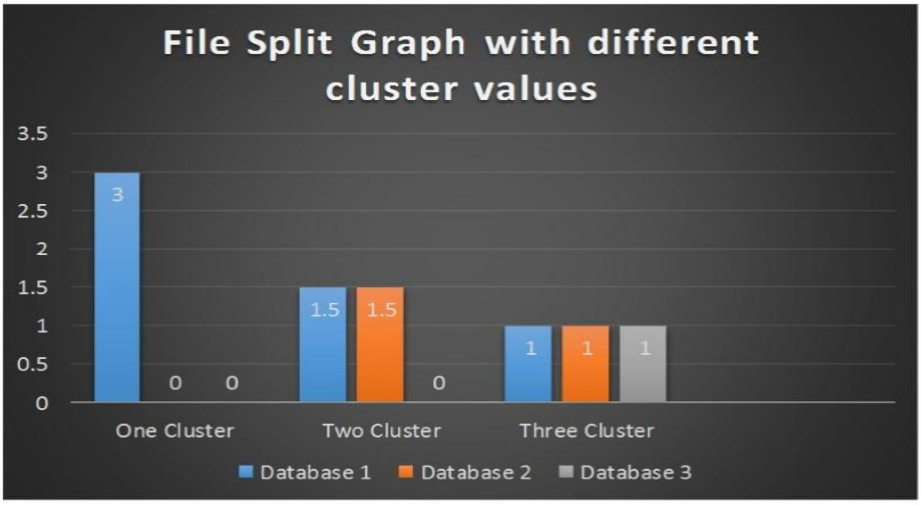
Decryption Time (in milliseconds)

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Graph evaluation of Split size



Graph Evaluation of Encryption and Upload time



CONCLUSION AND FUTURE WORK

IaaS is the establishment layer of the Cloud Computing conveyance demonstrate that comprises of numerous segments and innovations. We have proposed a system that will provide better security in cloud environment. We have proposed a security architecture which provides strong security using AES algorithm. The proposed system provides better time efficient solution and security in cloud environment. In future we plan to provide more security to system using multiple encryption algorithm at ones. We also plan to provide file sharing feature in the system so that user will be able to share their file. We will also like to provide an extra feature of data availability which will help increase

reliability of system even if one of the server crashes.

REFERENCES

[1] Cloud Computing Security: From Single To Multi-Clouds Mohammed A. Alzain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference On System Sciences.

[2] Ensuring Data Integrity And Security In Cloud Storage Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.

[3] Reliable Re-Encryption In Unreliable Clouds Qin Liu ,Chiu C.Tan ,Jiewu, And Guojun Wang IEEE Communications Society Subject Matter Experts For Publication In The IEEE Globecom 2011 Proceedings.

[4] Service-Oriented Cloud Computing Architecture Wei-Tek Tsai, Xin Sun, Janaka Balasooriya 2010 Seventh International Conference On Information Technology

[5] Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014

[6] Mell-Peter, Grance-Timothy. September 2011. The NIST Definition Of Cloud Computing.

[7] C. Cachin, I. Keidar And A. Shraer, "Trusting The Cloud", ACM SIGACT News, 40, 2009, Pp. 81-86. Clavister, "Security in The Cloud", Clavister White Paper, 2008.

[8] H.Mei, J. Dawei, L. Guoliang And Z. Yuan, "Supporting Database Applications As A Service", ICDE'09:Proc. 25thintl.Conf. On Data Engineering, 2009, Pp. 832-843.

[9] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security In Cloud Computing", ARTCOM'10: Proc. Intl. Conf. On Advances In Recent Technologies In Communication And Computing, 2010, Pp. 1-9.

[10] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina And Eduardo B Fernandez An Analysis Of Security Issues For Cloud Computing Hashizume Et Al. Journal Of Internet Services And Applications 2013.

[11] Gehana Booth, Andrew Soknacki, and Anil Somayaji Cloud Security: Attacks and Current Defenses 8th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'13), JUNE 4-5, 2013, ALBANY, NY.

[12] Brent Lagesse Challenges In Securing The Interface Between The Cloud And Pervasive Systems IEEE Pervasive Computing, Vol. 8, Pp. 14–23, October 2009. [Online].

[13] Wayne A. Jansen Cloud Hooks: Security And Privacy Issues In Cloud Computing Proceedings Of The 44th Hawaii International Conference On System Sciences – 2011.

[14] Mukesh Singhal And Santosh Chandrasekhar Collaboration In Multicloud Computing Environments: Framework And Security Issues Published By The IEEE Computer Society 0018-9162/13/$31.00 © 2013 IEEE

[15] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.

[16] Lukas Malina and Jan Hajny Efficient Security Solution for Privacy-Preserving Cloud Services 6TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013

[17] Morgan, Lorraine Conboy, Kieran FACTORS AFFECTING THE ADOPTION OF CLOUD
COMPUTING: AN EXPLORATORY STUDY Proceedings of the 21st European Conference on Information Systems 2012

[18] Sarita Motghare, P.S.Mohod International Journal of Advanced Research In Computer Science Volume 4, No. 4, March-April 2013

[19] Bryan Ford Icebergs in the Clouds: The Other Risks Of Cloud Computing SIGCOMM, August 2010

[20] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.

[21] Abhinandan P Shirahatti, P S Khanagoudar Preserving Integrity of Data and Public Auditing For Data Storage Security In Cloud Computing IMACST: VOLUME 3 NUMBER 3 JUNE 2012

[22] Allan A. Friedman and Darrell M. West Privacy and Security in Cloud Computing Number 3 October 2010

[23] Mohamed Nabeel, Elisa Bertino Privacy Preserving Delegated Access Control in Public Clouds PUBLISHING YEAR 2012

[24] Myrto Arapinis, Sergiu Bursuc, and Mark Ryan Privacy Supporting Cloud Computing: Confichair, A Case Study University Of Birmingham Nov. 2012

[25] Darko Andročec Research Challenges For Cloud Computing Economics Nov. 2011

[26] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull Security Issues with Possible Solutions In Cloud Computing-A Survey International Journal Of Advanced Research In Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013