An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication (CSA) Protocol Suite

Tamilarasi R, Prabu S and Swarnalatha P
School of Computing Science and Engineering
VIT University, Vellore -632014

ABSTRACT

The main concern of cloud computing is security which providiesauthenticationto the data whichis stocked in the cloud environment. There are numerous studies on handling huge/large size of data in the cloud computing platform and it is also a big challenge in front of the cloud computing researchers,. Instead of handling or processing the large data set in the cloud, the data sets are segmented into pieces of facts and figures placed on the priority and confidentiality of the facts and figures. Hence, the segmentation ,i.e, partitioning method have been used to facilitate the Transformation of Secure Data and Images (DIMs) into Public Cloud Service(PCS). Along with that, Public Encryption Algorithm (an improvised AES) has been used to safeguard data security which will increase the key size(Shared Key). Also storage of data requires the involvement of Public Cloud Service Provider (PCSP). They come up with strong encryption security. After the storage of DIM Cloud-based Secure Authentication (CSA) protocol suite is used to make aware of Denial of Service (DOS) attacks. Based on the survey and study, the existing data protection security deals with two-tier architecture which involves security of DIMs. Therefore, this paper proposes a Three-Tier Architecture to provide improvised data protection along with high level of data security, authentication, confidentiality and prevents data leakage using segmentation and CSA.

Keywords:-Cloud Computing; Public Cloud DIMs Security; Authentication CSAProtocol Suite; Segmentation Techniques; AES; Three-Tier Architecture.

1. INTRODUCTION:

Cloud computing plays an important role in an IT and business area. It maintains many data's and Application in cloud service. Generally it is internet based computing to access the resources from anywhere any time. It is like "Pay and Use" approach.

In figure 1, the paper deals with the cloud computing a three service model that is Software as a Service(SaaS). In SaaS representationthe cloud supplier (provider) will set up and perform the application software in the cloud. The cloud user *retrieve* an application and database through internet connection which are from cloud client(mobile phone,thin client ,etc.). In Platform as a Service(PaaS)representationthe cloud provider delivers the cloud flatform which includes operating systems, programming language execution environment. Application developers develops and runs the software in a cloud infrastructure. An operator of the cloud need not worry about the price and difficulty for purchasing (or) orderingand handlingthe underlaying hardware and software. In Infrastructure as a Service(IaaS), service provider provision the computing resoures within provider infrastructure, which can be deployed and excuted using OS, Applications,etc. Thereby maintaining operating eqiupments. This paper deals with survey of related security issues in cloud computing such as Authentication ,Confidentiality and Data Leakage.

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

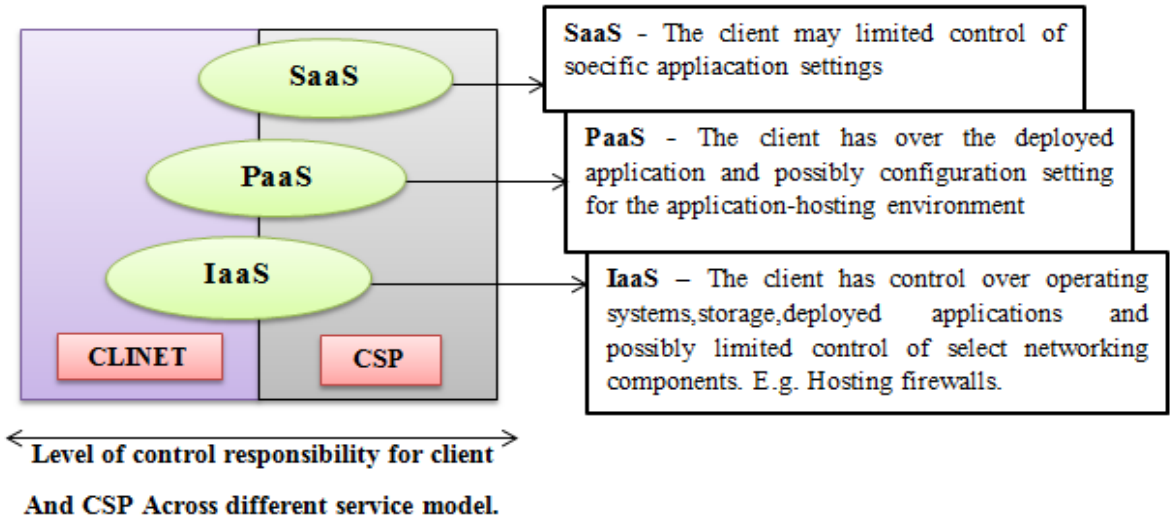

Figure 1: Sample Service Model

The paper is formulated as follows : Section2 Deals with Literature Survey on four techniques like Authentication,Segmentation,AES Encryption and Three-Tier Architecture. Section 3 Proposed Architecture. Section 4 Discuss about the Research Methodology. Section 5 Conclusion and Future Work.

2. LITERATURE SURVEY:

2.1 AUTHENTICATION:

Authentication techniques are used to protect the data's in cloud,Group Key Authentication Protocol(GKAP). It's a defined protocol that gives authentication data protection with sensible authentication period wherein data makes a mess of data traffic in the cloud computing and concurrently improve the Quality of Service(QoS) [1]. Digital Signature techniques also used in authentication process[2]. Self-Verified timestamp technique is used to avoid man-in-middle attack and supports Smart-Card-Based Authentication (SCBA)structure (which will not first efficiently succeed password-authenticated key agreement but also pass up the complexity of establishing clock synchronization in multi-server environments). Also in paper[3], a successful as well as appropriate remote password authentication scheme with key agreement was proposed. The paper [4] discuss with the view of strong user authentication structure in consideration of cloud computing with a lot of protection characteristics namely; identity management, mutual authentication,session key agreement among the consumer, the cloud server and user kindliness(i.e, Password modification level). Time-bound ticket-based mutualauthentication scheme isprojectedin paper [5] to overcome the unprotectionto Denial-Of-Service attacks and unconfident password alteration level.

2.2 SEGMENTATION:

One centermost consideration in cloud computing is secrecy and reliability of data developments in cloud. By reason two or more different clouds, consequences like control of data and one more fear attendant with procedure interference can be reduced. So to provide reliability and confidentiality, the application and data are partitioned into two different clouds in order that no cloud provider will improve the complete understanding of the user information(data).The controller performs

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

encryption and segmentation about the data to give data confidentiality[6]. Image segmentation is a method of partitioning an image into purposeful fields. Thereexist many digital image segmentation methods which are at present practiced on individual fields [7].Watershed algorithm [8] is an awfully great technique for image segmentation with the apply of mathematical morphology for cloud computing.

TABLE 1: Comparison of Various Encryption Algorithms:[9][10]

Features	**AES**	**RSA**	**DES**
Developed	2001	1997	1970
Key length	128,192 or 256	Variant	56
Block Size	128 bits	1024 bits	64 bits
Security Rate	Excellent	Good	Not Enough
Execution Time	More Fast	Slowest	Slow

2.3 AES (ADVANCED ENCRYPTION STANDARD):

AES is a Symmetric block cipher used by the U.S. government to secure confidential data and is implemented in software and hardware everywere to encryptimpressionable facts and figures. The size of a block of 128 bits, but three different key lengths:128, 192, and 256 bits. Its have shared key by using same key for both side. AES algorithm uses least time to execute cloud data.

The advantages of AES algorithm on comparison with RSA and DES algorithms with a tabular representation (table 2) as given below. The table discusses about the merits between 2007 to 2015 for better analysis of AES. This has led to an efficient Improvised AESalgorithm.

TABLE 2: Benefits of AES Algorithm over RSA and DES:

Year of Publications	**Benefits of AES Algorithm**
2007	The AES block cipher algorithms produces fitted and quick implementation and also itused for amount of data's encryption[11]
2008	It (AES) showed in efficient security increment across other ES methods. This needs to secure the information taken away malevolent (malicious) attacks uses Advanced Encryption Standard (AES), also known as Rijndael algorithm. It is used to develop hardware of AES Algorithm quickly which is more secured then software developments [12][13].

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

Year of Publications	Benefits of AES Algorithm
2009	AES is an advanced symmetric secret word encryption algorithms through its protection, flexibility and simple to use characteristics. It's used generally in Business Applications. The appliance of AES algorithm in auditing data safety can avoid Malicious larceny and escape of auditing data from inside to outside for safekeeping the protection of computing data's [14]. Here paper [15] present applicable digest values to each AES different transformation, which enables to secure each application objectively. from the scientific information of each AES specific transformation.
2010	AES provides suitable plain of information confidentiality and gives ultimately far superior security also. AES security framework also is used to perform authentication and encrypted data transfer to assigned data confidentiality [16]. A new algorithm of AES parallel encryption is a structured and developed a quickly data encryption system based on GPU (Graphics processing Units)[17].
2011	AES algorithm provide high level of security using medical image encryption which takes long time implementation. Here AES is used to secure the ROI region only [18].
2012	AES method aims to provide user achievement by transmitting personaland psychic DIM's securely [19].
2013	Using AES encrypted algorithm, cloud users information provides safety and security on comparison with other attacks. Implementing AES for security of data yields more advantages of decrease in less memory and less performance time compared to other algorithms[20].
2014	Advanced encryption standard algorithm and Visual cryptography is used to secure pathological Biometric images.AES cryptography algorithm is one of the best greatest algorithm as evaluated to other ES algorithms[21].
2015	AES for security in data provides less estimation time and utilization of memory. It alsogives safety and security in client information compared to other algorithms[22].

2.4 THREE-TIER ARCHITECTURE:

The papers[23][24] proposed three-tier secured data architecture that contains different levels of secrecy were dealt by clients. This paper surveyed the drawback(gap) of data leakage caused by cloud index in section 3.

3.PROPOSED ARCHITECTURE:

In the proposed architecture (fig.2), we have used four levels of protection structure.

- First level discuss about the Cloud based-secure Authentication (CSA) Protocol suite which is used to generate the authentication process.
    - Under this, CSA Protocol suite has been used with three step process like Registration Protocol, CSA Adaptive-Based Identification Protocol and Authentication Protocol (For CSA Protocol Suite, private cloud along has been considered for data only in SaaS [25]). But

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

in this paper we have proposed public cloud security for data and images (DIMs) in PaaS wherein Protocol Suite alone is not quite enough to proceed. These has made to proceed to second level.

- In second level, for extra security purpose, Improvised AES encryption algorithm has been proposed to increase the key level.
- The third level deals with the partitioning method that is used to divide the encrypt data and images(DIMs) in order to transfer into the public cloud server(PCS). Actually the protocol suite strictly aware of DoS attacks(internally and externally) through the three secure techniques which gives strong security for public cloud data and images(DIMs) in PaaS.

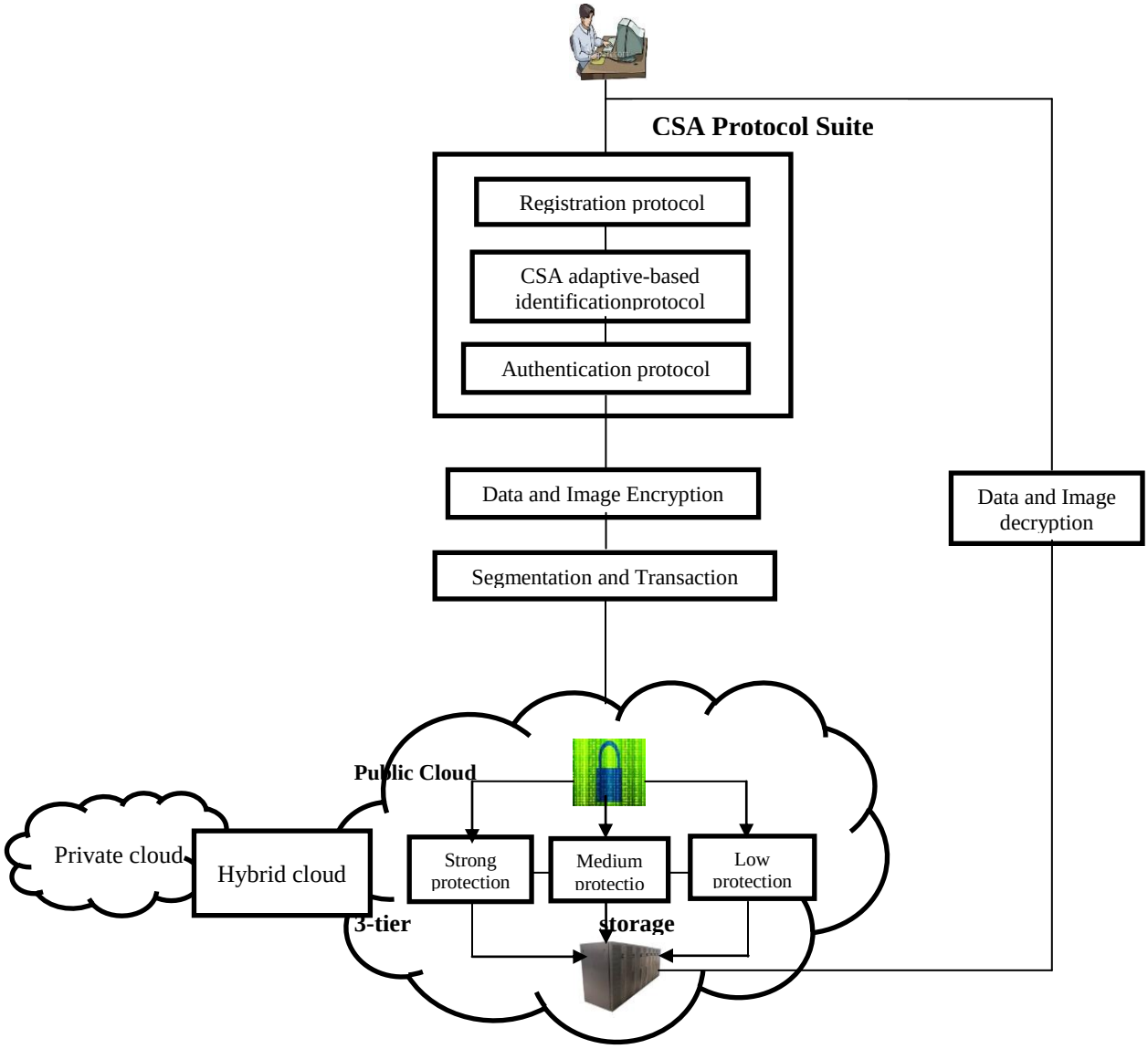

Figure 2: Proposed Architecture of Data and Image Security in Public Cloud

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

- The fourth level of the proposed architecture i.e., three tier architecture which fills the gap of data leakage.A detailed study on the proposed architecture is given in the section 4.

4.Analysis of Proposed Architecture

In this paper, the figure 2 deals with data and images (DIMs), a proposed architecture. It includes four security techniques as section 4.1 with cloud-based authentication protocol suite, AES Encryption technique in section 4.2, and Partitioning (Segmentation) technique in section 4.3 and three-tier data protection architecture in section 4.4 for prevention of data leakage.

4.1. Cloud-based Secure Authentication (CSA) Protocol Suite :

The paper [25] proposed an authentication protocol suite whichdetect and authenticate cloud users at SaaS layer and providessecureprotection in contradiction of DoS's attack in private cloud. In this private cloud data security purpose,the CSA protocol suite is used which provides authentication security. The CSA protocol suite can be implemented in the SaaS layer of cloud computing systems because the protocol basically relies on fundamental hardware and software provisionsof the cloud systems and cloud users. But when we store the data or images in the public cloud, we need more security for that.

Hence, in this work, we have proposed an CSA protocol suite to find a legitimate cloud user's at PaaS layer. But public cloud DIM's we proposed for security purpose, some other techniques(AES, Segmentation, Three Tier Architecture) also.CSA consists of three steps i.e., 1.Registration protocol,2.CSA adaptive-based identification protocol,3.Authentication protocol as explain in section 3

4.2. AES Encryption Algorithm :

The paper discuss with the AES encryption algorithm for DIM's security in public cloud server. It provides more security and confidentiality of data's as it will increase the key level. Normally AES algorithm gives excellent security for information. AES key size are 128, 192 or 256 bits. Increase in the key level gives strong security in public cloud information. Thereby the hackers never attack the DIM's.

4.3. Partitioning (Segmentation) Technique :

After encryption of the DIM's, the paper proposed a segmentation technique. This helps to divide the data to transfer the public cloud server which yields extra security process in the DIM's.

4.4. Three-tier data protection architecture for preventing data leakage :

The main aim to use this architecture is to avoid the data leakage and to protect the DIM's. The three tier architecture in which presentation,application processing and data management functions is displayed in figure 3.

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

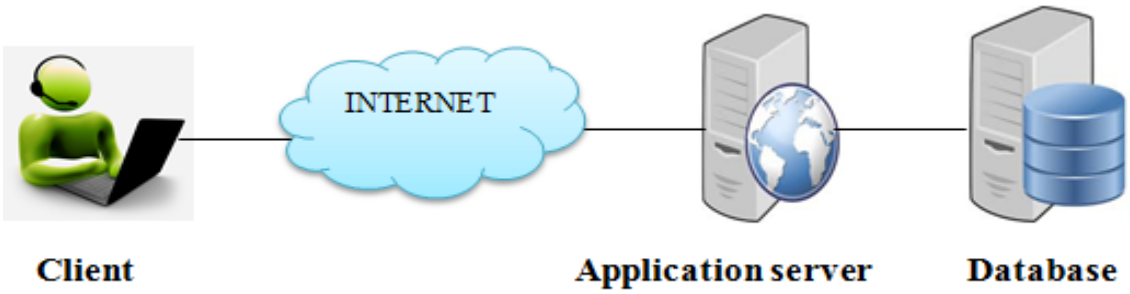

Figure 3 : Three tier Architecture

The figure 3 discuss 3-tier architecture which has three level data protection methods. They are Strong protection, Medium protection, Low protection.

4.4.1. Strong Protection :

The service supplier is not permitted to study the hypersensitive serving of the user's information. Therefore as to refute the threat of indexing being directed on sensitive serving of the file that might indicate to confidentialitylosses.

4.4.2. Medium protection :

The service provider is prevented from "effective" indexing. In commandent the objects of indexing is to run up the analysis of estimated data element across random approach. Once random approach is rejected, indexes will become unusable.consequently, the paper proposed an method to deactivate random approach to the data element in the customer's documents. Our method does not trust about connection mechanism policies.

4.4.3. Low protection :

The customer specifies visiblyin the policy scheme the management of his data documents and the usage of indexing. The service provider is expected reliable and will notify and consult with the user the keywords to be used for indexingbenefits.

5.CONCLUSION AND FUTURE WORK :

Based on the study, this paper concludes with improvised performance. Based on author proposed Data and Images (DIMs) Architecture to study and solve the data security problems like authentication,confidentiality, DIMs leakage and transaction in the cloud computing. Nowadays data security is a big challenge task in the public cloud. The Cloud-based Secure Authentication (CSA)Protocol Suite was already implemented in private cloud to handle the DoS attacks both internally and externally using data such as users information only.But still they could not provide an improvised security. Hence,this paper proposes an architecture using CSA protocol inpublic cloud for data with images (DIMs) also.The authors also proposes to introduce

an architecture to enhance the security with an AES encryption algorithm by increasing the key size.An increase in the key sizewill provide more security and confidentiality to the client data and the client images (DIMs). Another DIMs security mechanism of partitioning the data and images (encrypted format) to transfer into public cloud server. After the transfer,leakage problems will happen occur in the server side, to handle this an enhanced three tier-architecture protection method

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

is proposed to protect the data and prevents the leakage. As a whole, this paper proposes an enhnaced and an efficient security for DIMs using suitable data and image security techniques such as enhanced AES and, partitioning method in the public cloud.

REFERENCES :

1.Pradeep Kumar,K.Selvamani,S.Kanimozhi ,"An Authentication Approach for Data Sharing in Cloud Environment for Dynamic Group" 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT),Vol.pp.262-267,2014.

2. Prashant Rewagad,Yogita,"Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" 2013 International Conference on Communication Systems and Network Technologies,.pp.437-439,2013.

3.Woei-Jiunn Tsaura,Jia-Hong Lib,Wei-Bin Leeb,"An efficient and secure multi-server authentication scheme with key agreement " The Jurnal of System and Software,Vol.85,Issue 4,pp.876-882,April, 2012.

4. Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee,"A Strong User Authentication Framework for Cloud Computing" 2011 IEEE Asia -Pacific Services Computing Conference,Vol.74,pp.110-115,2011.

5. Jaidhar C.D," Enhanced Mutual Authentication Scheme for Cloud Architecture" 2013 3rd IEEE International Advance Computing Conference (IACC),pp.70-75,2013.

6. M Sulochana,Ojaswani Dubey," Preserving Data Confidentiality using Multi-Cloud Architecture" 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15),Vol.50,pp. 357-362, 2015.

7. Binamrata Baral, Sandeep Gonnade, Toran Verma," Image Segmentation and Various Segmentation Techniques – A Review" International Journal of Soft Computing and Engineering (IJSCE),Vol.4,Issue 1pp.134-139,2014.

8. Pinaki Pratim Acharjya, Dibyendu Ghoshal," Image Segmentation Technique for Cloud Computing Environment Using Morphological Approach" International Journal of Scientific & Engineering Research,Vol.4,Issue 8,pp. 1839-1839, 2013.

9. Chander Kani, Yogesh Sharma," Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3,Issue 5,pp.570-575, 2013.

10. Vanya Diwan1 , Shubhra Malhotra2 ,Rachna Jain,"Cloud Security Solution:Comparison among Various Cryptographic Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering,Vol.4,Issue 4,pp.1146-1148, 2014.

11. AJ Elbirt , Member, IEEE*," "* Fast and Efficient Implementation of AES Via Instruction Set Extensions" 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07),Vol.1,pp.56-69,2007.

12.[1]Md. Nazrul Islam, [1]Md. Monir Hossain Mia et.al., "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing .pp.291-294,2008.

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)

13. Jyothi Yenuguvanilanka, Omar Elkeelany,"Performance Evaluation of Hardware Models of Advanced Encryption Standard (AES) Algorithm" SoutheastCon(SoutheasrCon),2008 Proceedings IEEE.pp.222-225 ,2008.

14. Qing-xiang zhu1, lu li1, jing liu2, nan xu1,"The Analysis and Design of Accounting Information Security System Based on AES Algorithm" Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding. pp.2713-2718, 2009.

15. Laurie Genelle, Christophe Giraud and Emmanuel Prouff," Securing AES Implementation Against Fault Attacks" 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography.pp.51-62, 2009.

16. M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica"A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" International Journal of Computer Applications,Vol.12,Issue 8,pp.19-23, 2010.

17. Deguang Le, Jinyi Chang, Xingdou Gou, AnkangZhang, Conglan Lu,"Parallel AES Algorithm for Fast Data Encryption on GPU" 2010 2nd International Conference on Computer Engineering and Technology,Vol.6,pp.V6-1 – V6-6,2010.

18. Ahmed ,B.Mahmood, Robert, D.Dony," Segmentation Based Encryption Method for Medical Images" 6th International Conference on Internet Technology and Secured Transactions, pp.596-601,2011.

19. P.R.Radhadevil, P.Kalpana," Secure Image Encryption Using AES" IJRET: International Journal of Research in Engineering and Technology,Vol.01,Issue 02,pp.115-117,2012.

20. Abha Sachdev, Mohit Bhansali," Enhancing Cloud Computing Security using AES Algorithm" International Journal of Computer Applications,Vol.67,Issue 9,pp.19-23, 2013.

21. Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, J.M.Eghan, Nii Narku Quaynor," Feature Based Encryption Technique For Securing Forensic Biometric Image Data Using AES and Visual Cryptography" 2014 Second International Conference on Artificial Intelligence, Modelling and Simulation.pp.199-204, 2014.

22. Kiruthika.R, Keerthana.S, Jeena.R," Enhancing Cloud Computing Security using AES Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering,Vol.5,Issue 3,pp.630-635, 2015.

23.Anna Squicciarini, Smitha Sundareswaran, Dan Lin,"Preventing Information Leakage from Indexing in the Cloud" 2010 IEEE 3rd International Conference on Cloud Computing,.pp.188-195, 2010.

24. Poonam Sawdekar, Seema Shah," Implementation of Information Leakage Avoiding (ILA) Application in Cloud Computing" International Journal of Computer Applications,Vol.97,Issue 13,pp.54-57,2014.

25. Marwan Darwish,el.al.,"A Cloud-based secure authentication(CSA)protocol suite for defense against Denial of Service(DoS)" Journal of Information security and Applications,pp.1-9,2015.

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05)