Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

AN ARCHITECTURAL FRAMEWORK FOR SECURE CLOUD DATA STORAGE MANAGEMENT BY USING ORTHOGONAL HANDSHAKING AUTHENTICATION MECHANISM (OHSAM)

K.Subramanian[#1] and M.Mohamed Sirajudeen[#2]

[#1] *Department of Computer Science, Govt.Arts College, Pudukottai, Tamil Nadu, India.*
#2 Department of Computer Science, J.J College of Arts and Science, Pudukottai(dt), Tamil Nadu, India.

ABSTRACT :- *Cloud Computing is the promising inclination in the contemporary computing era and to provide an outstanding road map between demand and supply over the network. If the required data or information is available within the campus network server or service provider no way to focus on security about data residing in the server. At the same moment, the data or information sharing among a particular group is also never deliberate about security issues on data. When the issues go out of scope, is required to focus more and more on data security and its storage mechanism over the network. Based on this concern, the cloud data storage in third party network routinely comes under the high risk of security issues in the cloud storage management. In order to eliminate this drawback, different researchers proposed diversity of security algorithms combined with cloud computing mechanism. In spite of, most of the category its fail to fulfil the contemporary security threat on the cloud data storage. In this research paper focus on an analytical survey of existing security mechanism in cloud data storage and propose an effective secure mechanism in order to provide a high rating security on the cloud data storage.*

Key words: *Cloud, Data, Storage and Security.*

I. INTRODUCTION

In most of the circumstance, the data resides in cloud data server is secured with the help of cryptographic algorithms. The functional architecture for each and every security algorithm is based on its key (K) management with different mechanism. For example, if the cloud data storage is combined with private key crypto algorithms maintain same key for both encryptions (E) and decryptions (D) along with to maintain it's in secret manner. In contrast, the public key algorithms maintain separate encryption and decryption key as well as to make it any one of the key as public also never bring a significant impact on its secure mechanism. Among all the existing security algorithms (Julius Ceaser Cipher, Transposition Cipher, RSA, DES, MD5), the RSA (Rivest, Shamir, Aldimer) is used in many occurrences regarding to ensure the security of cloud data storage in effective and efficient manner [5]. The general layered architecture for cloud data storage management is depicted in the following diagram (Figure 1).
It comprises two major components are: Application Interface and Access Layer. The access layer play an interface between the security algorithms and cloud data storage and the application interface create a bridge between the data as well as the crypto-key mechanism with the security algorithms.

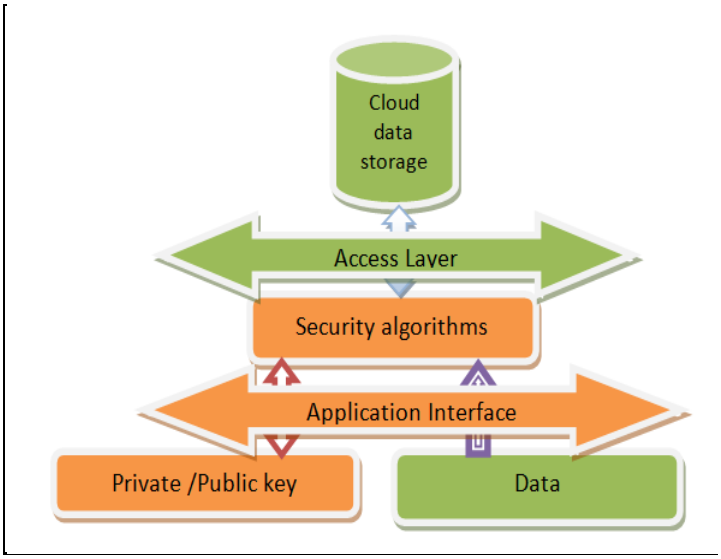

Figure 1 Security Mechanism in Cloud data storage Management

In general ,every aspect of data storage into the cloud server or cloud service provider follow certain storage mechanism such as sequential number generation , block allocation and the corresponding link address to indicate the succeeding memory locations. Ahead of to store into the cloud server, the data to be encrypted and occupy its appropriate location in the memory. The security algorithms play a vital role as an intermediate interface between the access layer and the application interface in order to establish a link between cloud storage and encryption data [2].
The following diagram (Figure 2), illustrate cloud memory storage architectural framework layout. Cloud service users or clients send their request to the cloud service providers (CSP) in order to get service for either one of the service offered by cloud such as: IaaS, PaaS and SaaS. The service approval is required to get an authentication from the Data owners in private cloud regarding to ensure its secure data communication over the network. In this architectural framework, the cloud servers are used to maintain the Block Allocation Sequential Link Table (BASLT) and security control flow towards the CSP [4].

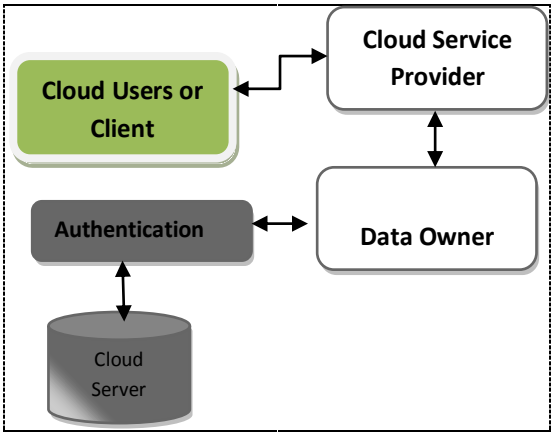

Figure 2. Cloud Storage Architecture (CSA)

The cloud storage architectural representation for different types such as: Private, public and Hybrid is exposed in the following diagrams (Figure 3, Figure 4 and Figure 5).

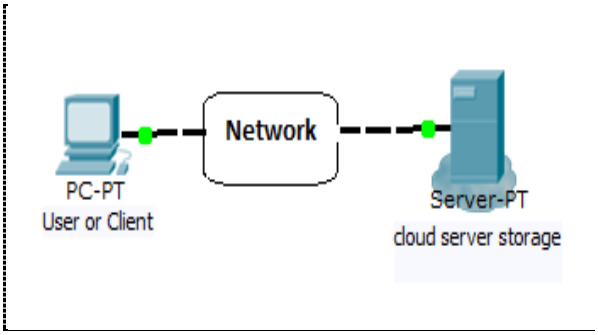

Figure 3.Private Cloud

In Private cloud storage access is carried out among the authorized group of users or clients in a secure way with the help of some standard cryptographic algorithms.

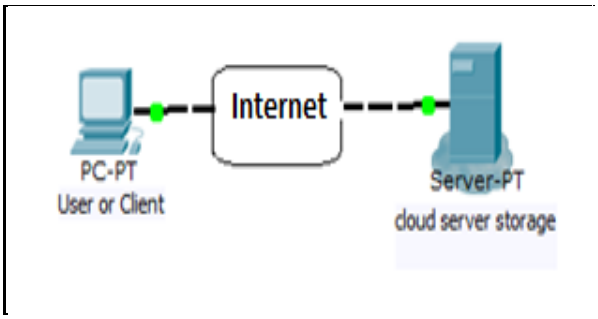

Figure 4. Public Cloud

At the same time, Public cloud get access request from different categories of users or cloud clients regarding to share unclassified data or information resides in cloud servers.

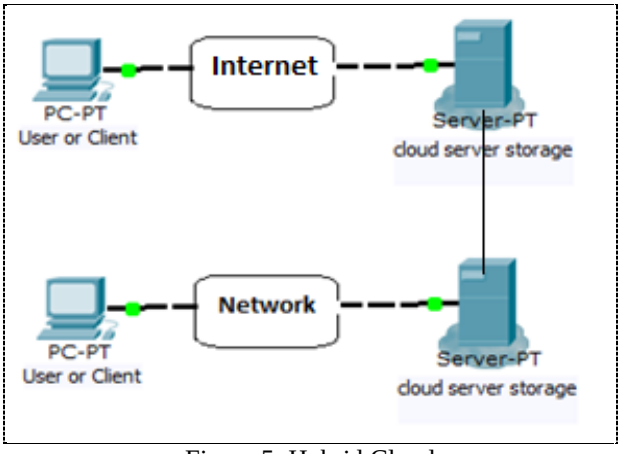

Figure 5. Hybrid Cloud

Both type of services are combined together in order to make it a part of protected one and the rest as unclassified or make it a public one is called as "Hybrid Cloud". Each and every types of cloud sharing with common storage characteristics are: Access Control, Performance, Scalability, Availability, Reliability, Security and Storage efficiency. Each and every researcher proposes security algorithms according to their perspective mainly focus on secure data transaction among the cloud service clients with the help of generalized encryption algorithms. But in this research paper give more attention on encryption mechanism of cloud data along with its key distribution management in an effective and efficient manner by propose a modern approach named as "Orthogonal Handshaking Authentication Mechanism (OHSAM).

I. RELATED WORK

In order to maintain the secure cloud data storage, the researchers propose different cryptographic mechanism on the stored data or before to provide towards clients or cloud users over the network [3].
Among the existing proposal , the most related work [1] here specified by introducing a different approach with the help of OTP (one time password) for authenticating appropriate users either in the storage request or access request over the network. Both Encrypted data and the Encryption key is existing in the same cloud storage or server. The working principle behind this OTP authentication system is clearly depicted in the following figure 6.

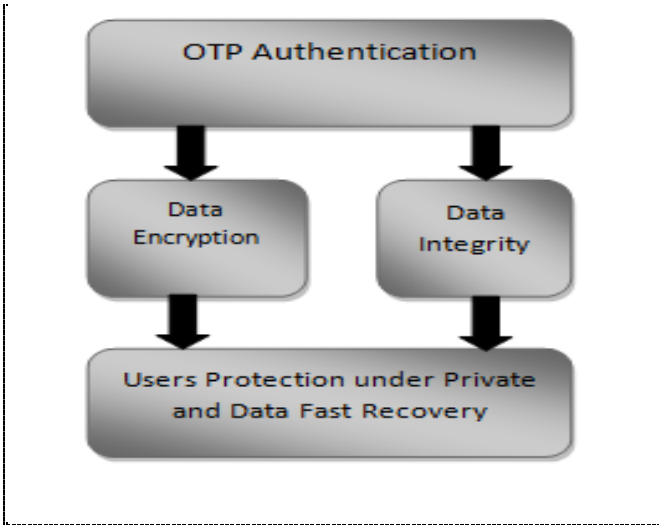

Figure 6. OTP Authentication in Cloud

The authentication is confirmed with the help of OTP request from the cloud server whenever the client or cloud user initiates their request regarding the data access. If the authentication phase successful progress to open the gateway for cloud data encryption along with integrate the encrypted data with encryption Key. Based on this mechanism it provides a secure cloud data in storage as well as transaction aspects over the communication channel. The following UML class and sequence diagram (Figure 7a, b) explains its detailed functional procedures in a summarized manner.

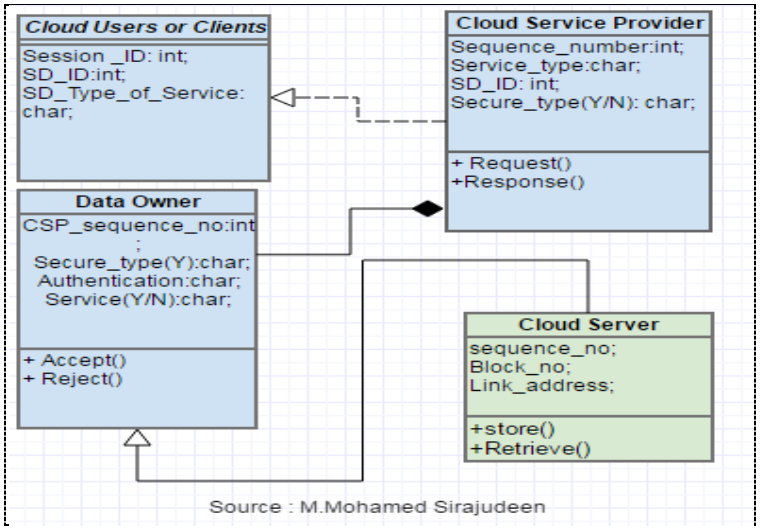

Figure 7 (a). Class Diagram for CSA

The Authentication requirement after receiving the request from cloud client is confirmed with the help of OTP. After get approval for successful authentication, to continue the related service with the interaction between cloud client and cloud server. The major drawback of this mechanism is to get an OTP in different interval of time and some occasion the cloud client not able to get due to the slow internet connection or poor network. Even though, if the client is an authenticated person in order to interact with the cloud server create a problem for unauthorized access manner. The Encryption data also easily breakup by the intruders with the help of encryption key binding with its content and resides same cloud server.

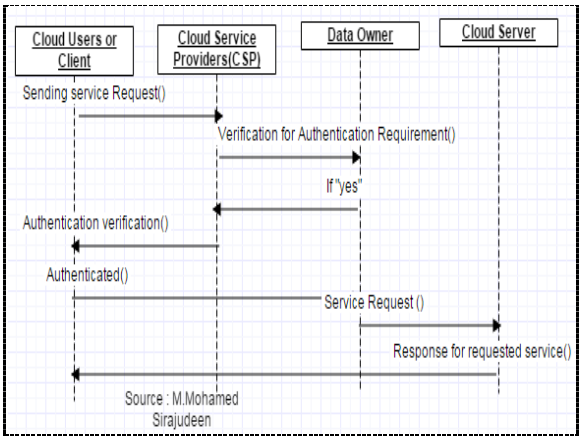

Figure 7(b). Sequential diagram for OTP authentication

In a different perspective of another one researcher [2] propose , the secure cloud architectural storage frame work based on the authentication by using digital signature for each and every storage block (B) in cloud server [Figure 8] .

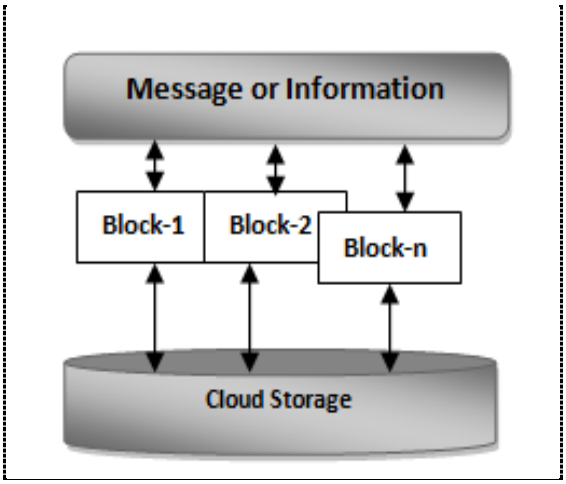

Figure 8. Cloud Storage framework by using blocks9B)

Initially, the entire message or data is divided into a number of discrete blocks (B). Instead of authenticating each and every individual data or message packets over the communication channel, this approach is used to perform a group of certain bit length messages or data together in to a block (B) [4]. At the moment, every block using certain authentication procedure in order to provide a cloud service as secure manner through the network. The outline of authentication algorithm by using block structure is given below,

Procedure Block_Authetication ( )

Step 1: Divide the original data or message (M) into fixed size of Packets (S).
Step 2: Group the specified number of packets into a Block (B) as a fixed size or variable –length size.
Step 3: Assign the authentication code from any one of cryptographic algorithms.
Step 4: Do the authentication process by using the key (K) at the time of receive any request from cloud clients or users.
Step 5: If the Authentication process is success, then provide the service, otherwise to terminate from the request.

The following flowchart (figure 9), obviously describe the Block_Authentication ( ) of secure cloud data storage,

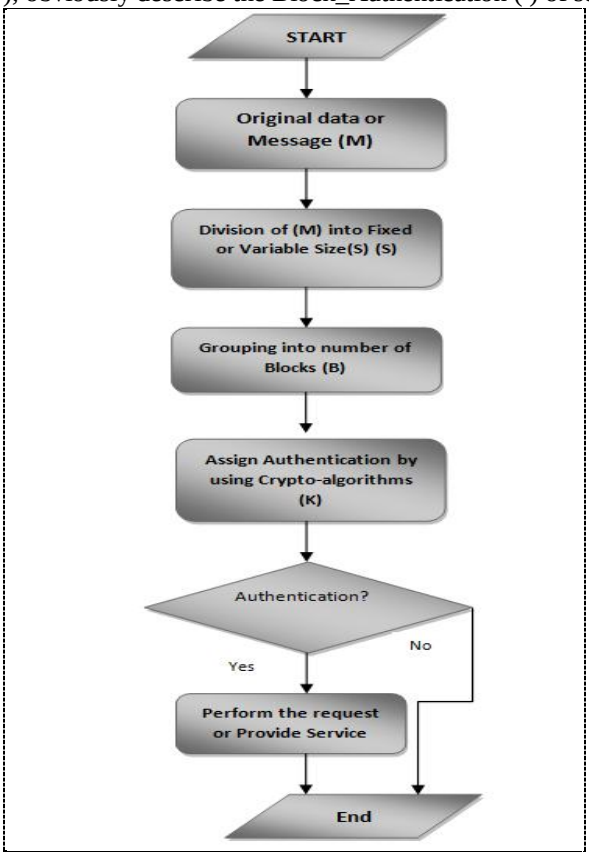

Figure 9. Flow Chart for Block_Authentication mechanism in Cloud Storage

II. PROPOSED WORK

The proposed research work focus on secure cloud data storage management in a uniqueness manner by using a modern approach of Orthogonal Handshaking Authentication Mechanism (OHSAM). It encompasses three components are: Working Principle, Architectural Layout and Data Storage Mechanism.

A. Working Principle (WP) :

In general, the orthogonal working principle is based on selective object or segment in perpendicular with each other. Let us consider the an informal group of physical address for each and every cloud server (CS) in the following diagram (figure 10), creates an orthogonal matrix (OM) as follows,

$$OM(CS) = \begin{Bmatrix} CC:1012 & AA:1010 \\ DD:1013 & BB:1011 \end{Bmatrix} \quad (1)$$

$$OM(CS) = \begin{Bmatrix} AA:1010 & CC:1012 \\ DD:1013 & BB:1011 \end{Bmatrix} \quad (2)$$

From the given example, If the cloud service consider the origin in left most and bottom of existing cloud servers, then the physical address CC: 1012 is perpendicular with BB: 1011 as well as the physical address DD: 1013 is perpendicular with AA : 1010 (in equation 1) . In the same characteristics, if it considers the origin is right most and the bottom of existing cloud server, then the physical address AA: 1010 is perpendicular with BB: 1011 as well as the physical address DD: 1013 is perpendicular with CC: 1012 (in equation 2). It also satisfy the another orthogonal property of transposition (OT). The combination of orthogonal selection is initiated with the help of handshaking authentication mechanism.

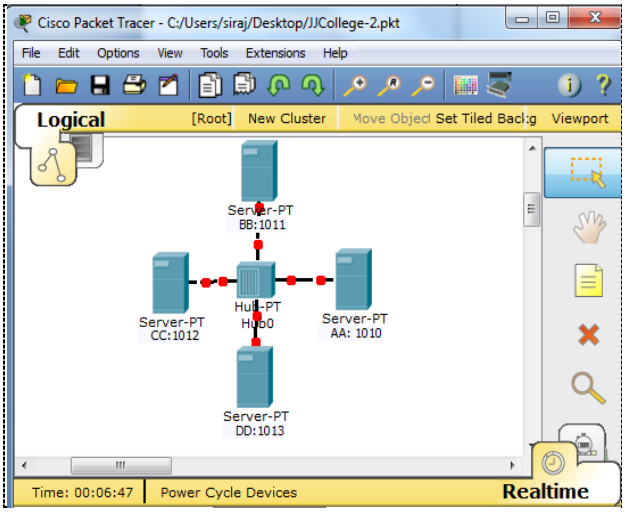

Figure 10. Orthogonal working Principle

B. Architectural Layout (AL) :

The road map of secure cloud data storage primarily focuses on the base of orthogonal working principle as well as its selection mechanism (Figure 11). Each and every cloud server to be found in cloud infrastructure is segmented into an orthogonal blocks and their physical address are grouping in a separate linking table named as "Orthogonal Block Link Table (OBLT)" with the attributes of Name of the Origin cloud server with its physical address, its size of Data storage (initially to be considered a unknown value such as "XXX") and the Link of succeeding one.

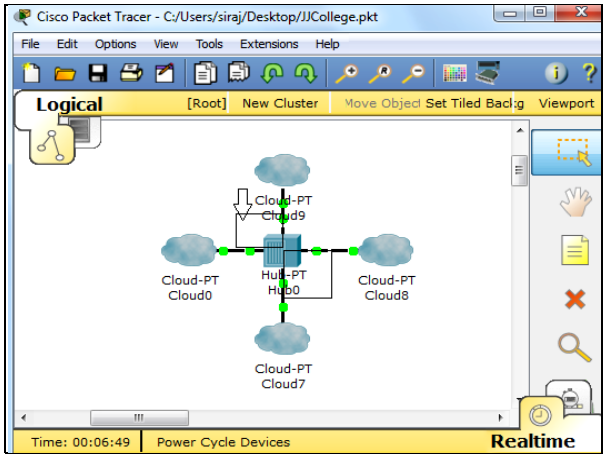

Figure 11. Architectural Layout for OHSAM

For example, let us consider the physical address for existing four cloud servers with its physical addresses are AA: 1010, BB: 1011, CC: 1012 and DD: 1013 (Figure 10). If the originating of service is left most and bottom of existing cloud servers, then the physical address CC: 1012 is perpendicular with BB: 1011 as well as the physical address DD: 1013 is perpendicular with AA: 1010 (in equation 1) is representing by using the following OBLT (Table 1),

Table 1. Layout for Orthogonal Block Link Table (OBLT)

Name of Origination cloud server with its physical address	Size of Data Storage	Link of Succeeding Cloud Server
CC: 1012	**XXX**	**BB: 1011**
DD: 1013	**XXX**	**AA: 1010**

C. Data Storage Mechanism (DSM) :

In broad-spectrum, the data or information are store into the cloud server a well known mechanism of either a block of plain text or block of cipher text by using any one of the encryption algorithm and retrieved with the help of an encryption key. But, in this proposed approach the data or information is fragmented into different size of packets and every packet having its own sentence structure (Figure 12).

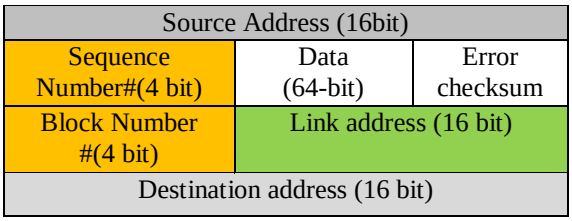

Figure 12. Packet Layout for Cloud Storage

The source and destination addresses are usually represent for data owner's IP address and the cloud service provider IP address respectively. In the case of fragmentations of original data is describing with the attributes of sequence number of the packet as well as the block number for the cloud server storage. The field of Link address is used to identify the location of its continuation of block in the cloud server over the communication network. The field of Error check sum is used to represent if errors free or not over the communication channel.

III. CONCLUSION

In this Research paper, provides a proposed layout for secure data storage mechanism in cloud servers with the help of a new approach named as "Orthogonal HandShaking Authentication Mechanism (OHSAM)". The expansion with the functional architectural framework for data serving and localization principles under cloud infrastructures will continues in the future work. This mechanism ensures the secure cloud data storage and access by the cloud clients in secure manner without any complication.

REFERENCES

[1]. Ashwini Banasode, Megha Singh, " Implementation of Cloud Storage Security Mechanism using Digital Signature", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 1, January 2015. ISSN: 2277128X, Pp. 956-960.

[2]. Allen Oommen Joseph, Jaspher W.Kathrine, Rohit Vijayan, "Cloud Security mechanism for Data Protection: A survey", International Journal of Multimedia and Ubiquitous Engineering, ISSN: 1975-0080, Vol.9, No.9 (2014), Pp: 81-90, http://dx.doi.org/10.14257/ijmue.2014.9.9.09.

[3]. Eman. M.Mohamed, Hatem S.Abdelkader, "Data Security model for cloud computing", ICN 2013: The Twelfth International Conference on Networks, ISBN: 978-1-61208-245-5.

[4]. Cai Zehua, Wang Shunyan, Long shangyin, Zhhou Haitao, " A data storage and Management Scheme in Cloud storage model" in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013). Page no: 2397-2400.

[5]. Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing Using RSA Algorithm", International Journal of Research in Computer and Communication Technology, ISSN: 2278-5841, Vol 1, Issue 4, September 2012. Pp 143-146.

