Design and Implementation of Secure VSN Multi-cloud Storage Model

Mr.Amit R.Gadekar
Ph.D Scholar ,Dept. Computer Engg
SITRC, Pune, India

Dr. M V.Sarode
Department of Computer Engineering
Government Poly., Yavatmal India

Dr.V M.Thakare
Department of Computer Engineering
SGBAU,Amravati

Abstract : Cloud Computing is a new computing model that distributes the computing missions on a resource pool that includes a large amount of computing resources. More and more companies begin to provide different kinds of cloud computing services for Internet users at the same time these services also bring some security problems.

Internet users are able to acquire computing resource, storage space and other kinds of software services according to their needs. In cloud computing, with a large amount of various computing resources, users can easily solve their problems with the resources provided by a cloud. Today most cloud computing system use asymmetric and traditional public key cryptography to provide data security and mutual authentication. This Paper helps in securing the data without affecting the original data and protecting the data. In this technique the data are segmented into three different levels according to their data importance ranking, set by data owner. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is to store data in a secure and safe way in order to avoid intrusions and attacks. Also, it will reduce the cost and time to store the encrypted data in the Cloud Computing. The thesis conducts a performance analysis by implementing the Advanced Encryption Standard (AES) in all levels in order to check the performance of model.

Index Terms— Advanced Encryption Standard ,Cloud Computing, Security, VSN.

1. Introduction

Cloud Computing has been growning significantly as well as become one of the most important areas of Paper in the recent years. Cloud distributes the computing missions on a resource pool that includes a large amount of computing resources. It is the result of development of infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS),With broadband Internet access, Internet users are able to acquire computing resource, storage space and other kinds of software services according to their needs. In cloud computing, with a large amount of various computing resources, users can easily access resources provided by a cloud. This brings great flexibility for the users, using cloud computing service; users can store their critical data on servers and can access their data anywhere from the geographical location by using the Internet and no need to worry about system breakdown or disk faults, etc. Also, different users in one system can share their information and work, as well as play games together. Hierarchy identity-based cryptography is the development key to solve the scalability problem. Recently identity-based cryptography and hierarchy identity-based cryptography have been proposed to provide security for some Internet applications. Cloud computing allows user to store large amount of data in cloud storage from any part of the world via internet by using any terminal equipment. As we know that cloud computing is rest on internet, there are security issues occurred like data security, confidentiality and privacy. In order to resolve these problems, various types of encryption algorithms and techniques are used. Many Paperers used and found the best techniques with different combination to provide security to the data in cloud. In this synopsis Secure Data Partitioning Technique and cryptography algorithms are used to protect confidentiality of data stored in cloud.

.

2. Literature Review

Wireless In Cloud computing, there are set of important policies, which include issues of privacy, anonymity, security, liability and reliability, M. Sulochana, Ojaswani Dubey [1] Cloud Computing offers resources as services that are dynamically provisioned over the internet. The security of cloud computing has always been an important aspect of the quality of service from cloud service providers. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. Orner K. Jasim Mohammad, SafiaAbbas, EI-Sayed M. EI-Horbaty [2] proposed a Comparative Study between Modern Encryption Algorithms based On Cloud Computing Environment.This work provides a comparative study that represents the differences between modern encryption algorithms in cloud computing (DES, 3-DES, AES, RC4). D. S. Abdul. Elminaam [3] stated a Performance Evaluation of Symmetric Encryption Algorithms AES, DES, 3DES, RC2 and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Zhonghua Sheng Zhiqiang Ma Lin GuAng Li [4] proposed A Privacy-Protecting File System on Public Cloud Storage to provide strong protection on user data. C. Selvakumar G. JeevaRathanam M. R. Sumalatha [5] Improving Cloud Data Storage Security Using Data Partitioning Technique, the partitioning method is proposed for the data storage which avoids the local copy at the user side by using partitioning method.

K.Prabha S.Nalini [6], A Secure Data Forwarding in Cloud Storage, Forwarding operation performs by the re-encryption key. Each storage server uses the re-encryption key to re-encrypt its word symbols. Lan Zhou, Vijay Varadharajan, Michael Hitchens [7] Integrating Trust with Cryptographic Role-based Access Control for Secure Cloud Data Storage propose a trust model to reason about and improve the security for stored data in cloud systems that use cryptographic RBAC schemes. David S. L. Wei, Siani Pearson, Kanta Matsuura, Patrick P. C. Lee, and Kshirasagar Naik, Senior Member, IEEE [8] Guest Editorial: Cloud Security, investigate the fundamental properties of cloud security issues, including data auditing, searchable data encryption, hypervisor protection, cloud forensics, and disaster recovery. Natasha Saini,Nitin Pandey, Ajeet Pal Singh [9] stated Enhancement Of Security Using Cryptographic Techniques, The mechanisms includes: Integrity, Availability, Authentication, No repudiation, Confidentiality and Access control . Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE [10] Security and Privacy-Enhancing Multi-cloud Architectures, Security challenges are still among the biggest obstacles when considering the adoption of cloud services. Kan Yang, Xiaohua Jia, Kui Ren [11] DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems, Data access control is an effective way to ensure the data security in the cloud. HazilaHasansuriayatiChuprat [12] Secured Data Partitioning In Multi Cloud Environment, the concept of data partitioning, the current state-of-the-art of data partitioning and secured data partitioning in multi cloud environment is mentioned & then compared the current security approaches used to secure data partitioning in multi cloud environment.

3. Contributions

The contribution of this work has many fold: Implementation of novel Algorithm to reduce the cost of computation and storage, also improve the security in comparison with the existing methods . Implementation of hybrid cryptographic approach along with file splitting and merging mechanisms.

4. Proposed Work

The proposed papers aim is to provide enhanced security through data partitioning , encryption techniques & implementing it on multi-cloud storage rather than storing complete file on single cloud system. It will split the file in different chunks then encrypt and store them it on different clouds. The Meta data required for decrypting and rearranging a file and it will be stored in metadata management server.

This work proposed Secure Data Partitioning Technique to make data secure with less encryption time and storage space, for that the data are segmented into three different levels such as top-secure, secure & ordinary data according to their data ranking importance, these ranking is set by their data owners. The data in each secure level is encrypted by using encryption/decryption algorithms and keys before storing them on the cloud. The aim of this system is to store data in a secure way in order to avoid attacks and intrusions. It will also reduce the cost and time of storing the encrypted data on the cloud data storage center. This system overcomes the disadvantages of the existing system. In this system the file owner can decide the data permission of the file hence protecting the data from unauthorized access. The file is encrypted using the encryption algorithm thus confidentiality is maintained. The system is secure against the data theft attacks. The file is divided into smaller chunks and stored on multiple clouds to reduce the risk downtime due to a localized hardware, software, or infrastructure failures in a cloud-computing environment. The file is merged and decrypted when requested by the authenticate user.

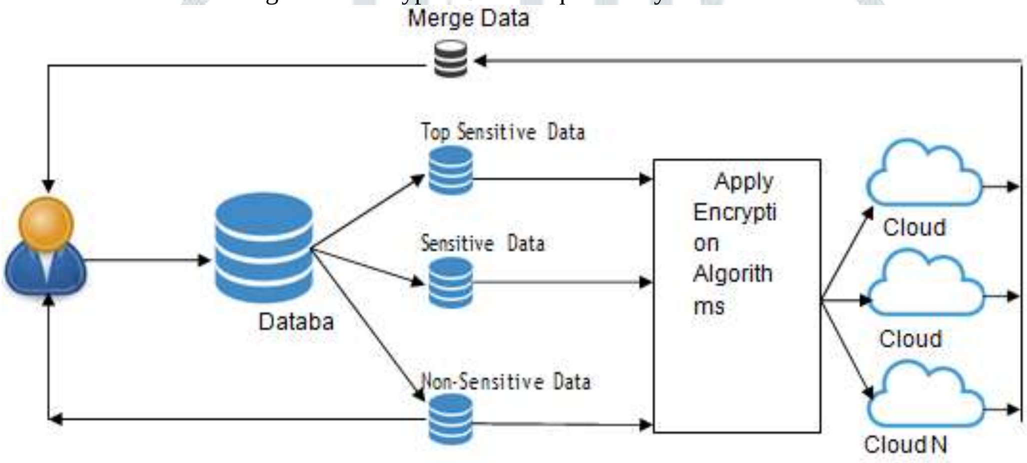


Figure 1: VSN Model

Data-Segmentation Technique

There are many ways to partition the huge data into set of proper and manageable size, such as vertical or horizontal segmentation, hybrid (horizontal and vertical), and database segmentation into subsets depending on specific criteria. Data varies from field to another field, so the data owner has responsibility for data classification to appropriate subsets according to their importance, depending on specific parameters, such as the following:

1 The degree of protection and security required for each dataset or group
2 The required size for each group.
3 The data size that generated after encryption.
4 The time required to store /retrieves each dataset.

Security Standards

There are many encryption algorithms used to protect the data, some of these algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Blowfish and other. Also, when talking about any encryption algorithms it means these are algorithms same as used to decrypt the encrypted data. In this work different encryption algorithms will be used to protect the high important data.

5. Security Analysis

Attacks on cloud data is increasing day by day with various techniques. Table 1 shows the idea about threats, attacking type with layer where it occurs mostly.

Threats	Attack type	Layer
Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed.	SPI
Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI

Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [28].	SPI
Data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application [29,30]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S
Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [31,32].	I
Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [29].	I
VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploiting some hypervisor vulnerability) [33,34]	I

Table 1: Cloud Threats

6. Result Analysis

In this section , three different Modules are to be Implemented

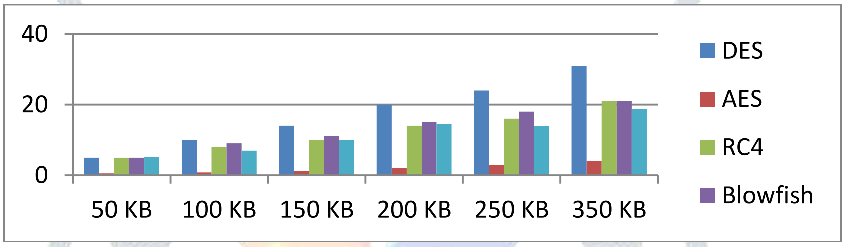
Module-I: Implementation of Cryptographic Algorithms for Performance Measurement in Cloud Computing

In this module, Symmetric and Asymmetric Cryptographic Algorithms are implemented on Local and Cloud machine , also according to the results ,best algorithm from set of algorithms are taken into consideration for further modules .

1. Implementation of Symmetric cryptographic algorithms.

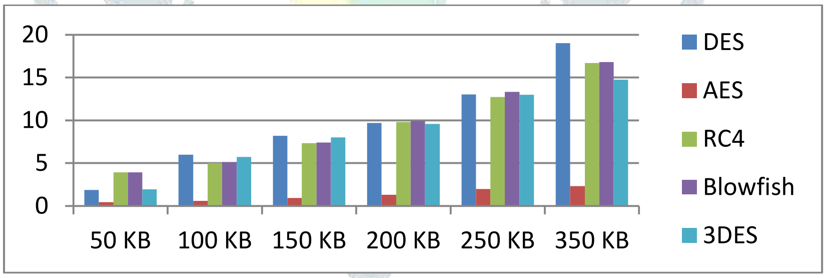
➢ Running time for symmetric algo. On single processor (Local Machine)

➢ Core i3 (3.4 Ghz) with 4 GB RAM with 300 GB-HDD

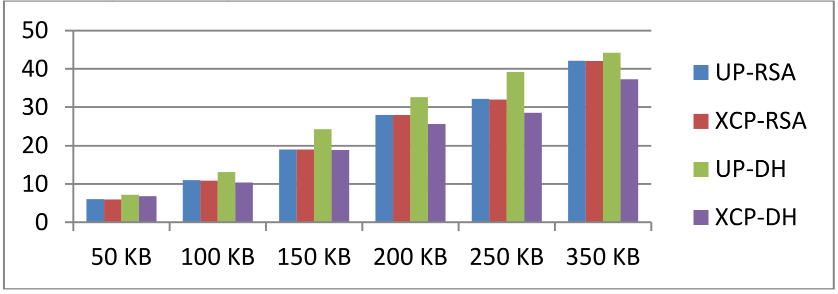


2. Running time for symmetric algo. On XCP (Cloud Machine)

➢ Core i5 (4.8 Ghz) with 16 GB RAM with 500 GB-HDD



➢ Running time for Asymmetric algo. On Single Processor and XCP (Cloud Machine)



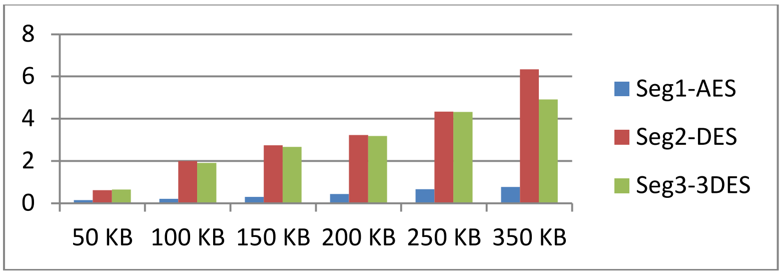
Module-II: Implementation of Hybrid-Cryptographic Algorithms for Performance Measurement in Cloud Computing

In this module, Symmetric and Asymmetric Cryptographic Algorithms are implemented on Local and Cloud machine but here the data is split into three parts according to user need, splitting of data is according to how much data is vital or how much data is sensitive ,also according to the results ,best algorithm from set of algorithms are taken into consideration for further modules.

1. Implementation of Symmetric cryptographic algorithms.

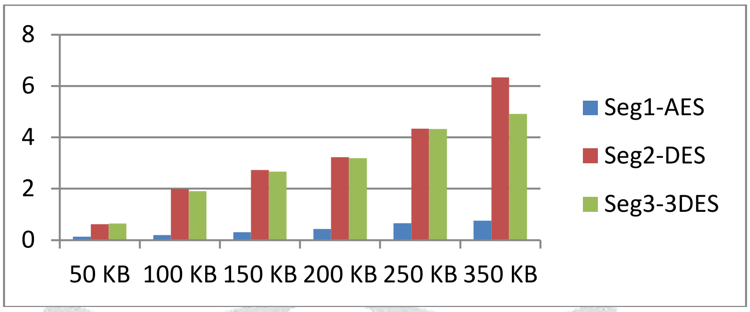
➢ Running time for symmetric algo. On single processor (Local Machine)

➢ Core i3 (3.4 Ghz) with 4 GB RAM with 300 GB-HDD

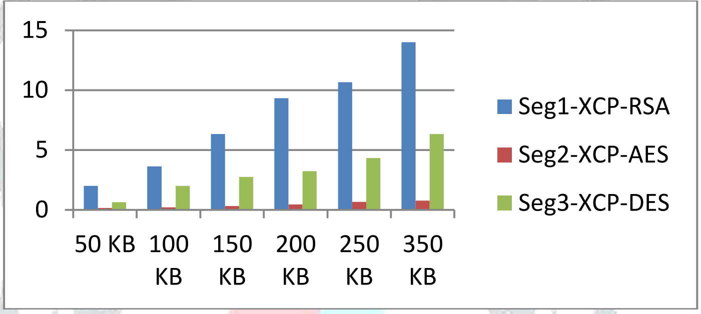


2. Running time for symmetric algo. On XCP (Cloud Machine)

- Core i5 (4.8 Ghz) with 16 GB RAM with 500 GB-HDD



- Running time for Asymmetric and symmetric algo. On XCP (Cloud Machine)



Conclusion from Module-I and II

1. Implementation of Symmetric cryptographic algorithms

- After segmenting the data, running time of the data transformation on the cloud network is faster than the running time on the local machine.
- After segmenting the data, there is an inverse proportion relation between the running time and the size of the input file. Such that, the increase of the input file size led to the decrease of the running time.
- After segmenting the data, AES is the fastest symmetric technique since it enjoys the scalability based on different hardware, as well as it can be implemented simply. After then, the symmetric techniques can be ordered as 3-DES, DES.

2. Implementation of Hybrid cryptographic algorithms on Cloud

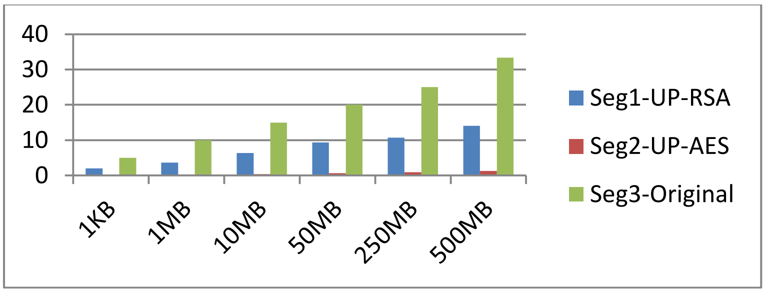
- The symmetric encryption techniques are faster than the asymmetric encryption techniques. Moreover, all algorithms in both categories (symmetric and asymmetric) enjoy the inverse proportion relation between the running time and the input file size, except the RSA algorithm.
- After segmenting the data and comparing with asymmetric algorithms, it is observed that AES is the fastest symmetric technique since it enjoys the scalability based on different hardware, as well as it can be implemented simply.

Module-III: Implementation of VSN Model for Performance Measurement in Cloud Computing

VSN model is based on Vital-data, Semi-vital-data and Non-vital-data. In this VSN Model dataset is divided into three segments ,as in Module-II we divided the data into three segments and all segments were encrypted using some cryptographic algorithms , but in this VSN we will not encrypt Non-vital data segment for the sake of reducing the encryption time, reducing the owners cloud service cost, and providing the suspension to Big Data problem. As per discussion in module I & II about implementation of Symmetric and Asymmetric Cryptographic Algorithms on Local and Cloud machine with data non-segmenting , segmenting according to user need or as per sensitivity level, some combination of hybrid cryptographic algorithms are taken into consideration for final implementation, for the best combination of algorithms which will be the best for top security .

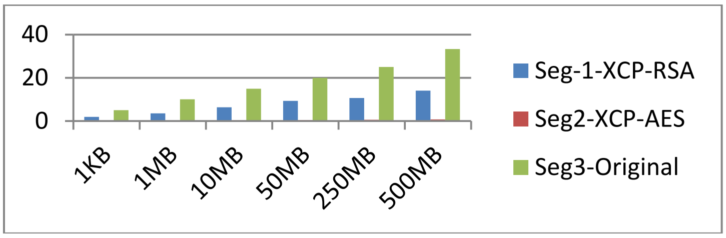
1. UP-VSN Model: Implementation of Hybrid cryptographic algorithms.

- Running time for Hybrid cryptographic algorithms on single processor (Local Machine)
- Core i3 (3.4 Ghz) with 4 GB RAM with 300 GB-HDD



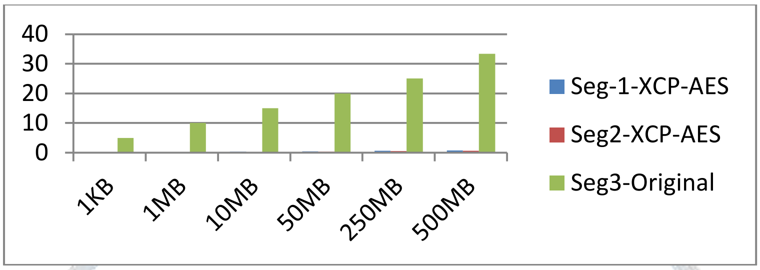
2. XCP-VSN Model: Implementation of Hybrid cryptographic algorithms.

- Running time for Hybrid cryptographic algorithms on XCP (Cloud Machine)
- Core i5 (4.8 GHz) with 16 GB RAM with 500 GB-HDD



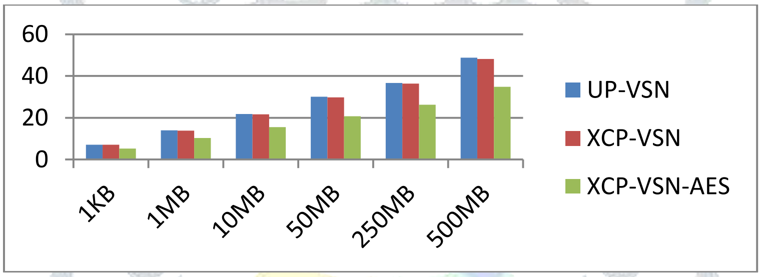
3. XCP-VSN-AES Model: Implementation of Hybrid cryptographic algorithms.

- Running time for Hybrid cryptographic algorithms on XCP (Cloud Machine)
- Core i5 (4.8 GHz) with 16 GB RAM with 500 GB-HDD



4. Comparison of Three versions of VSN Models

- Running time for Hybrid cryptographic algorithms on XCP (Cloud Machine)
- Core i5 (4.8 GHz) with 16 GB RAM with 500 GB-HDD



Conclusion from Module-III

1. UP-VSN Model: Implementation of Hybrid cryptographic algorithms

- After segmenting the data using VSN, AES is the fastest symmetric technique since it enjoys the scalability based on different hardware, as well as it can be implemented simply.

2. XCP-VSN Model: Implementation of Hybrid cryptographic algorithms

- The symmetric encryption techniques are faster than the asymmetric encryption techniques. Moreover, all algorithms in both categories (symmetric and asymmetric) enjoy the inverse proportion relation between the running time and the input file size, except the RSA algorithm.
- After segmenting the data using VSN and comparing with asymmetric algorithms, it is observed that AES is the fastest symmetric technique.

3. XCP-VSN-AES Model: Implementation of Hybrid cryptographic algorithms

- The AES symmetric encryption techniques are faster than the asymmetric encryption techniques as per results from previous two versions of VSN.. Moreover, AES combination for all segments or for sensitive data would be the best choice.

4. Comparison of Three versions of VSN Models

The symmetric encryption techniques are faster than the asymmetric encryption and the combination of AES for all segments has various advantages from all factors.

7. Conclusion

Cloud computing have many advantages in cost reduction, resource sharing and time saving for new service deployment. This Paper conducted some experiments on cloud security and its storage. This scheme proposed that, the data are segmented into three different levels according to their data importance ranking. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this Paper the aim is to store data in a secure and safe way in order to avoid intrusions and attacks. The experimental results show that, this proposed scheme efficient to reduce the cost and time to store the encrypted data in the Cloud Storage. In proposed work, a VSN Model is found to be secure and can provide the better security to specific applications with proper combinations of cryptographic algorithms. The computation and communication costs of the VSN Model are comparable with the existing related schemes. In addition, the proposed scheme also provides better security against different kind of attacks as compared to other existing related schemes.

REFERENCE

[1] M Sulochana, Ojaswani Dubey, " Preserving Data Confidentiality using Multi-Cloud Architecture", 2nd International Symposium on Big Data and Cloud Computing(ISBCC'15), ELSEVIER, Science Direct, pp.357-362, 2015

[2] Orner K. Jasim Mohammad, Safia Abbas, EI-Sayed M. EI-Horbaty , "A Comparative Study between Modern Encryption Algorithms based On Cloud Computing Environment", IEEE 8th International Conference for Internet Technology and Secured Transactions, pp.531-535,London,2013

[3] D. S. Abdul. Elminaam, H. M. Abdul Kader, "Performance Evaluation of Symmetric Encryption Algorithms " , Communications of the IBIMA, ISSN: 1943-7765, Volume 8, IEEE, pp.58-64,2009

[4] Zhonghua Sheng Zhiqiang Ma Lin GuAng Li, "A Privacy-Protecting File System on Public Cloud Storage",International Conference on Cloud and Service Computing, 978-1-4577-1637-9,IEEE,pp. 141-149, 2011

[5] C. Selvakumar G. JeevaRathanam M. R. Sumalatha ,"PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique", IEEE, pp. 7-11, 2012

[6] K.Prabha, S.Nalini, "A Secure Data Forwarding In Cloud Storage", IEEE Proceedings of International Conference on Optical Imaging Sensor and Security, Coimbatore, Tamil Nadu, India, July2-3 , 2013

[7] Lan Zhou, Vijay Varadharajan, Michael Hitchens, "Integrating Trust with Cryptographic Role-based Access Control for Secure Cloud Data Storage", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 560-569, 2013

[8] David S. L. Wei, , Siani Pearson, Kanta Matsuura, Patrick P. C. Lee, and Kshirasagar Naik, Senior Member, IEEE, " Guest Editorial: Cloud Security", IEEE Transactions On Cloud Computing, Vol. 2, No. 4, pp. 377-379, October-December 2014

[9] Natasha Saini ,Nitin Pandey, Ajeet Pal Singh, "Enhancement of Security using cryptographic Techniques", 9781-4673-7231-2/15, IEEE Computer society, 2015

[10] J.M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi-cloud Architectures," IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, pp. 212-224, July/August 2013

[11] Kan Yang, Ren, Xiaohua Jia, Bo Zhang, and RuitaoXie, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", IEEE, pp. 1-12, 2013

[12] HazilaHasan, SuriayatiChuprat, "Secured data partitioning in multi cloud environment", Fourth World Congress on Information and Communication Technologies (WICT), IEEE, pp. 146-151, 2014

[13] Yawei Zhao, Yong Wang,"Partition-based cloud data storage and processing model", IEEE 2nd International Conference onCloud Computing and Intelligent Systems (CCIS), pp. 218-223, 2012