Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Multi Round Selective Encryption using AES Over Storage Cloud

Amanpreet Kaur[1] and Gaurav Raj[2]

[1] Lovely Professional University, India

Received: 14 April 2013 Accepted: 30 April 2013 Published: 15 May 2013

Abstract

Cloud computing is the re-incarnation of the client-server architecture. It is highly promising technology because of its unlimited resource provisioning and data storage services which help us in managing the data as per requirements. Due to the use of internet and vital remote servers to maintain the data and applications, the cloud computing environment becomes open for the attackers to attack on the user data and communication services. This paper mainly focuses on the user authentication and data security over the Broker Cloud Computing Paradigm by purposing new cryptographic technique named as Multi Round Selective Encryption using AES. Along with this, we compared our approach with existing cryptographic techniques as AES, Blowfish and Selective encryption to find out its pros and cons. The Multi Round Selective Encryption with AES is the best suitable technique where the file size is large because it gives fast execution by maintaining the encryption complexity as compared to selective encryption technique in public and hybrid cloud.

Index terms— AES, blowfish, selective encryption, storage cloud.

1 Introduction

loud Computing means that the applications are delivered to customers as services over the Internet. The hardware and systems software are held in the datacenters that provide those services. The services offered by the cloud computing have long been referred to as Software as a Service. The datacenter with hardware and software is known as Cloud. Cloud computing can be seen as the requirement of three users which are categorized as: a) End User End User just wants to use the application software's such as Ms Office, Paint Brush, and Image Processing Software etc. This sort of service is provided by Software as a Service model of cloud computing which gives freedom to the user from getting license of software.

2 b) Commercial Organization

A commercial organization who wants to spread his business with the help of website then he/she has to set up the servers and maintenance of servers which leads to the high cost. But the cost of infrastructure can be removed by having Infrastructure as a Service model of cloud computing because the storage and security of data, maintenance of servers etc is handled by the cloud service provider.

3 Cloud Computing Architecture Layers

On the bases of services cloud computing architecture can be categories as platform, infrastructure and software. These services are delivered and consumed in real time over the internet via web2.0 enabled web browser.

4 Software as a Service

It offers you easy access to various online applications that are being hosted on the infrastructure of a service provider.

5 Platform as a Service

Peas allows the end users in undertaking multiple functionalities like testing, different operating system, queuing management, developing, integrating, managing and securing cloud infrastructure and cloud apps. Author ? Research Scholar Department of Computer science and Engineering Lovely Professional University, Phagwara, India. E-mail : aman_kaler05@hotmail.com Author ? : PhD Scholar Punjab Technical University Kapurthala, India. E-mail : er.gaurav.raj@gmail.com Author ? : Professor and Head of CSE Department SUSCET, Tangori, India. E-mail : hodcse@suscolleges.com :

6 h) Deployment Models of Cloud Computing

The deployment models can be categorized by some features which can answer the following queries i.e.

1. Who owns the infrastructure? 2. Who manages the infrastructure? 3. Where is the infrastructure located? 4. Who accesses the cloud services?

7 Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

8 j) Private Cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

9 k) Hybrid Cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

10 II.

11 SECURITY ISSUES IN CLOUD COMPUTING

a) Loss of Goverance By using cloud infrastructures, the client necessarily cedes control to the cloud provider (CP) on number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.

12 b) Lock-In

There is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled. c) Isolation Failure Multi tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants. However it should be considered that attacks on resource isolation mechanisms are still less numerous and much more difficult for attacker to put in practice compare.

13 d) Compliance Risks

Investment in achieving certification may be put at risk by migrating to the cloud.

1. If the cloud provider cannot provide evidence of their own compliance with the relevant requirements. 2. If the cloud provider does not permit audit by the cloud customer (CC).

14 e) Management Interface Compromise

Customer management interfaces of a public cloud provider are accessible through the internet and mediate access to larger set of resources and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

15 f) Data Protection

Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of the data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place.

16 g) Insecure or Incomplete Data Deletion

When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping off data. Adequate or timely data deletion may also be impossible, either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

17 h) Malicious Insider

While usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include cloud provider system administrators and managed security service providers. reliability and availability, for cloud computing (RAS issues), and give appropriate, available and feasible solutions for some of them. As a result, Moving toward cloud computing require to consider several parameters and most important of them is security.

18 III. Related Work

Haying Live, Yin Hub et al. (2011) introduces cloud computing concepts and main features and analyzes the security of cloud computing and the security strategies are proposed for security issues related to cloud computing [5].

Mohammed Abdulla if Alizarin and Eric Paraded et al. (2011) discuss the issues of cloud computing database sharing and the security concern of the organizations. For this he proposes a secret sharing key based technique over the encryption. He discusses how we can secure the data by sharing the key to the database by distributing the keys over the entire network to different servers [15]. For retrievals, the query will be created by the single (nearest) receiver that will collect information from the servers and hence find a way to actual data. In his words, the encryption creates an overhead over the query response time by calling decryption routine that requires additional resources. He has proposed this scheme by using NetDB2 database engine. He compares the storage and retrieval of data by using the built in encryption routines that increased the response time due to decryption process involved. The data can be distributed over the network and can be used as spatial data for information retrieval. However he does not throw any light on large files and no-numeric data.

19 IV. Purposed Multi Round Selective Encryption using AES over Storage Cloud

Multi Round Selective encryption technique is updated version of the Selective encryption. Here, we provide freedom to the user for selection of rounds by using multiple indexes to improve performance in encryption process complexity for large size data storage in cloud. I.e. Medical Reports, Blue prints of big architectural designs etc. It is the most promising solutions to increase the speed of encryption as compared to the full encryption. Selected data after encryption becomes more secure against the attacks and it is fast. We have defined use of multi rounds in 11 steps as followed algorithm using AES.

20 Multi Round Selective Encryption (MRSE) Algorithm

1. Key Expansion Round keys are derived from the cipher key using Irondale's key schedule. 2. Initial Index Selection-In this we are taking the value of initial index as static value and thereafter we are getting the data in multiples of the selected initial index.

Volume XIII Issue III Version I advantages. Its security insufficiency and benefits need to be weighed before making a decision to implement it. Medico Jensen, Jorge Schwann, Nils Gruschka and Luigi Lo Icon et al. (??009) present a selection of issues of cloud computing security. It is investigated that ongoing issues with application of XML signature and the web services security frameworks, discussed the importance and capabilities of browser security in the cloud computing context i.e. Seas, raised concerns about cloud service integrity and binding issues (Peas) and sketched the threat of flooding attacks on Cloud Systems (Iasi) [14]. Cloud security issues focus primarily on data safety, data confidentiality and data privacy and discuss mostly organizational means to overcome these issues. In this paper, an overview on technical security issues of cloud computing environments. Starting with real world examples of attacks performed on cloud computing systems; give an overview of existing and upcoming threats to cloud computing security. Cloud computing also raises severe concerns especially regarding the security level provided by such a concept. Completely depending on the own data and carrying out task to an outside company, eventually existing in another country with a different regulatory environment, which may insist companies not to consider Cloud Computing but to stick to conventional local data. Craig Gentry of IBM et al. (??010) provides solution to the data security which is stored with a CSP. He proposes homoorphic encryption technique which states that the keys should be distributed over the network nodes and the data should be kept under multi-level encryptions [4]. For knowing the data, a user will have to use K-1 keys and further the node values where these keys have been stored by the client. At every node hierarchy will be maintained and at each of the hierarchical level, different algorithm can be applied. In this way no one will never ever be able to use the data without authenticity. Gentry proposed Lattice based data encryption for cloud. Same era Abdurrahman Lamella, Chan Year Yuen et al. (2011) discuss challenges regarding three information security concerns: integrity, confidentiality and availability. Most of the organizations are very much concerned about the ownership of their data. They address not only security challenges for cloud computing including Identity and Access Management(IAM) but also present authorization ,the current state authentication and auditing of users accessing the cloud along with emerging IAM protocols and standards [18]. Their main concern is to discuss some of the security IAM protocols used to protect cloud users and to conclude which of these protocols will be best for organizations which are moving in the direction of consuming the cloud services.

Farad Sabah et al. (2011) discussed the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines [17]. They summarize security issues, 3. Find out the size of data in number of bits and select the bits in the multiple of index value such as an initial index=2 and multiples of 2 i.e. 4,6,8??., So we will select the bits as 2 nd , 4 th ,6 th ??, n th bit where n is the last multiple of selected indexed value in the data. 4. Number of Rounds-User must specify the no. of rounds, how much time user would like to execute the whole process.

21 V. Results and Analysis

The table 1.1 depicts the comparison between the four cipher techniques with different size of files. In this table, the file size after encryption is almost similar for AES and Blowfish Algorithm while Selective AES and Multi Round Selective AES Algorithms have similar results in terms of file size with the negligible difference. Among all the encryption schemes, the file size increases for the encryption files as the size of original file increased.

22 Basis of File Size

The table 1.2 depicts the comparison between the four cipher techniques with different execution time to process the files. In this table, the execution time after encryption is the highest for AES, Blowfish Algorithm has come up with second highest point while.

23 VI. CONCLUSION

As from the table 1.1 and 1.2 we concluded that the Multi Round Selective AES is faster than AES and Blowfish, with more complex result than Selective AES. As the file size of Selective AES and Multi Round AES is equal, hence the transmission time of Selective AES and Multi Round AES Algorithms will be same. Therefore Multi Round Selective AES Algorithm is better than Selective AES in terms of security and better than AES as compared to private cloud and we need an algorithm which is secure as well as fast. So it is preferable to apply Multi Round Selective Encryption Algorithm in public and private cloud.

In the future, the researchers can make these improvements to make this technique better. 1. When the size of data is increased then its computation time is increased, one can decrease computation time by using appropriate methods. 2. Along with this, the control overheads increased at large scale due to excess encryption and decryption of data. 3. Due to large encryption and decryption process the large amount of power is consumed, therefore one can ebb the power consumption. and Blowfish Algorithm in terms of the speed. As we know that over the public cloud there is more congestion [1]

[1] © 2013 Global Journals Inc. (US) Global Journal of Computer Science and Technology

Figure 1: Figure

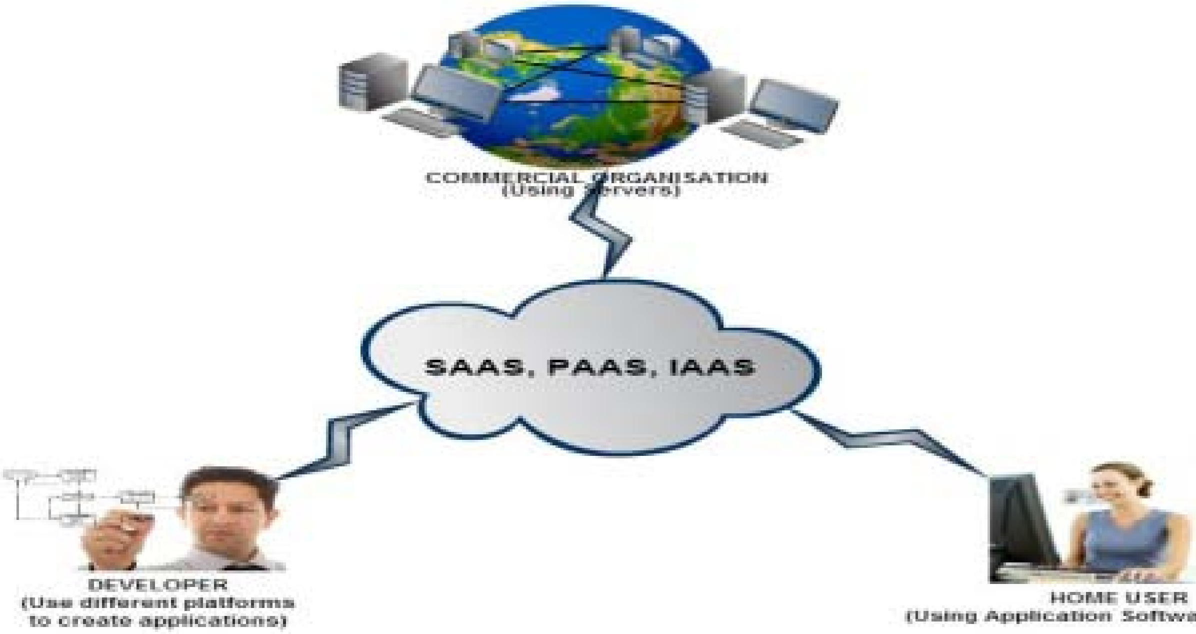
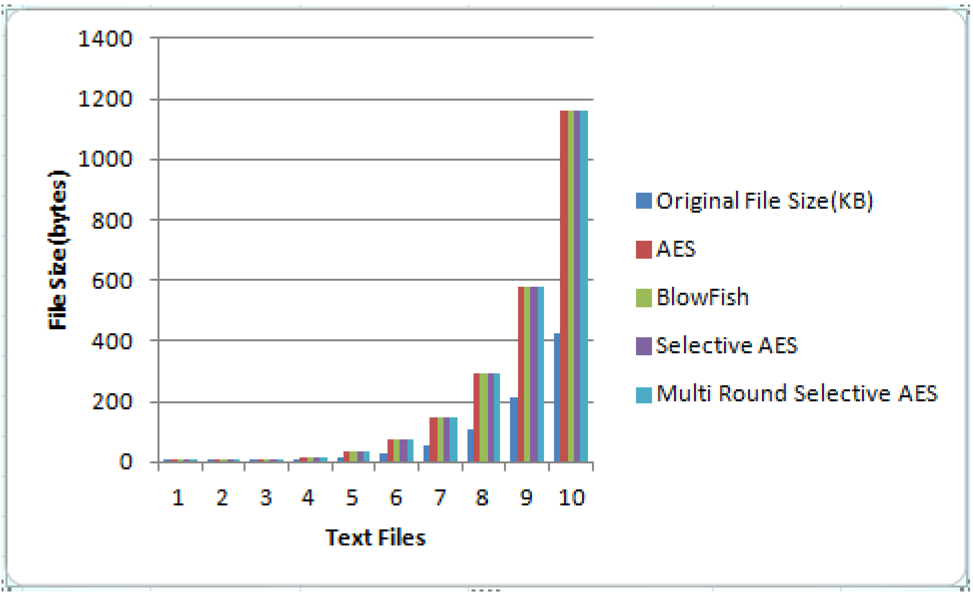
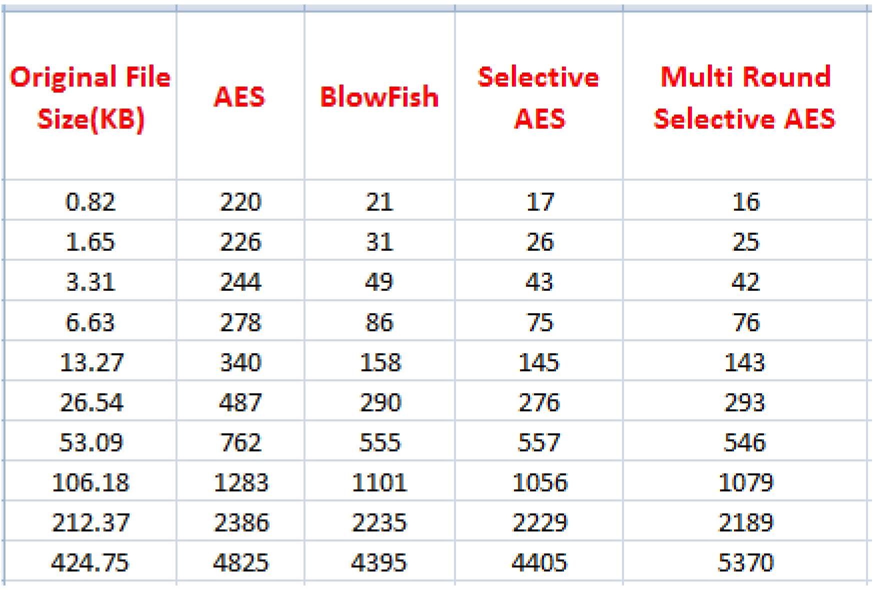


Figure 2:



2

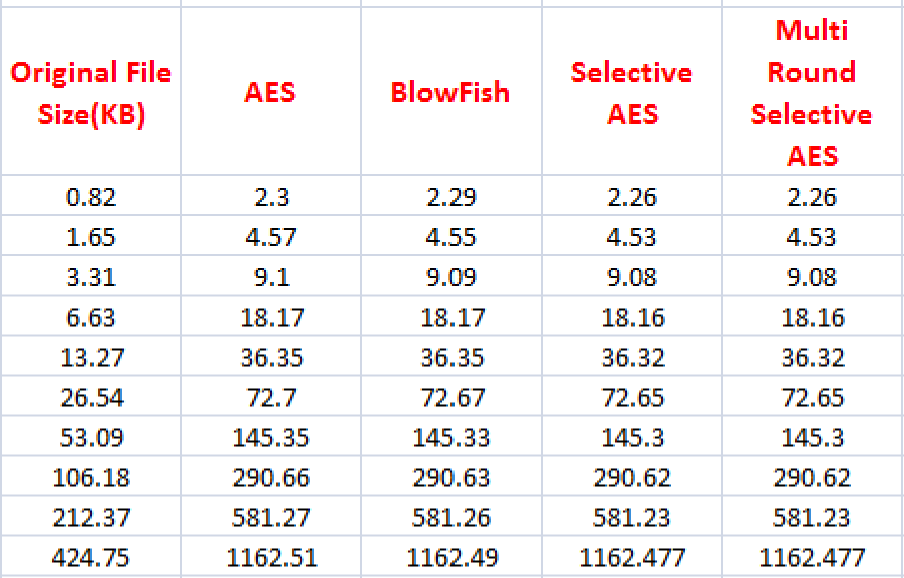
Figure 3: Train 2 B



Original File Size(KB)	AES	BlowFish	Selective AES	Multi Round Selective AES
0.82	220	21	17	16
1.65	226	31	26	25
3.31	244	49	43	42
6.63	278	86	75	76
13.27	340	158	145	143
26.54	487	290	276	293
53.09	762	555	557	546
106.18	1283	1101	1056	1079
212.37	2386	2235	2229	2189
424.75	4825	4395	4405	5370

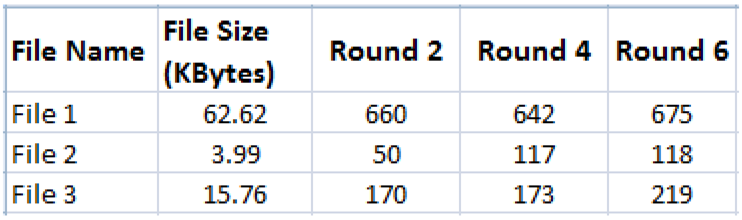
2

Figure 4: 2 B

5


Original File Size(KB)	AES	BlowFish	Selective AES	Multi Round Selective AES
0.82	2.3	2.29	2.26	2.26
1.65	4.57	4.55	4.53	4.53
3.31	9.1	9.09	9.08	9.08
6.63	18.17	18.17	18.16	18.16
13.27	36.35	36.35	36.32	36.32
26.54	72.7	72.67	72.65	72.65
53.09	145.35	145.33	145.3	145.3
106.18	290.66	290.63	290.62	290.62
212.37	581.27	581.26	581.23	581.23
424.75	1162.51	1162.49	1162.477	1162.477

Figure 5: 5 .



File Name	File Size (KBytes)	Round 2	Round 4	Round 6
File 1	62.62	660	642	675
File 2	3.99	50	117	118
File 3	15.76	170	173	219

Figure 6:

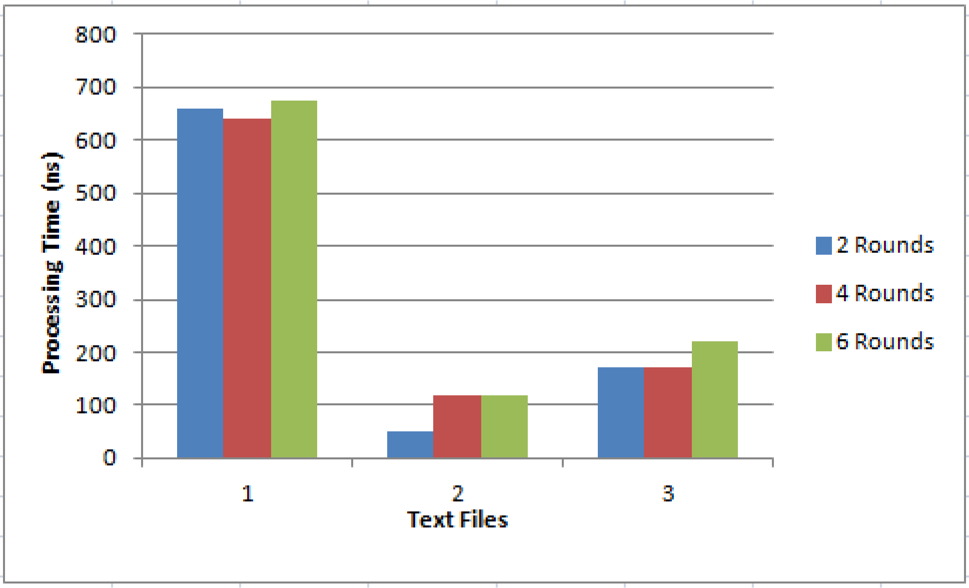
12


Figure 7: Figure 1 . 2 :

12

Figure 8: Table 1 . 2 :

1

Figure 9: Table 1 .

13

[Note: : Comparison of Muse Encryption Schemes on the Basis of Processing Time at Different Number of Rounds Figure 1.4 : Processing Time if Multi Round Selective Encryption Different No. of Rounds]

Figure 10: Table 1 . 3

[Cloud Environment. International Journal of Computer Applications] , *Cloud Environment. International Journal of Computer Applications* p. .

[Gentry ()] , C Gentry . 2009.

[Sudha ()] *A Comprehensive Approach to Ensure Secure Data Communication Communication Software and Networks*, M Sudha , DR . 2010. IEEE. p. .

[Mehmet Yildiz ()] 'A Layered Security Approach for Cloud Computing Infrastructure'. J H Mehmet Yildiz . *10th International Symposium on Pervasive Systems, Algorithms and Networks*, 2009. IEEE. p. .

[Kamal Dahbur ()] 'A survey of risks, threats and vulnerabilities in cloud computing'. B M Kamal Dahbur . *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*, (the 2011 International Conference on Intelligent Semantic Web-Services and Applications) 2011. ACM.

[Haoyong Lv ()] 'Analysis and research about cloud computing security protect policy'. Y H Haoyong Lv . *International Conference on Intelligence Science and Information Engineering*, 2011. IEEE. p. .

[Balachandra Reddy Kandukuri ()] R P Balachandra Reddy Kandukuri . *Cloud Security Issues. International Conference on Services Computing*, 2009. IEEE. p. .

[Yu ()] 'Cloud computing and security challenges'. Huiming Yu , NP . *50th Annual Southeast Regional Conference*, 2012. ACM. p. .

[B ()] 'Cloud computing Benefits, risks, recommendations for information security cloud computing'. B , R . *ENISA* 2009.

[Sameera Abdulrahman Almulla ()] *cloud computing security management. Engineering systems management and its application*, C Y Sameera Abdulrahman Almulla . 2011. p. .

[Sumter ()] 'Cloud computing: security risk'. L Sumter . *Proceedings of the 48th Annual Southeast Regional Conference*, (the 48th Annual Southeast Regional Conference) 2010. ACM.

[El-Etriby ()] *Computing, Modern Encryption Techniques for Cloud*, Sherif El-Etriby , EM . 2012. p. .

[Kaur ()] 'Implementing DES Algorithm in Cloud for Data Security'. N J Kaur . *VSRD International Journal of Computer Science & Information Technology* 2012. p. .

[Mahajan ()] 'Implementing Various Encryption Algorithms to Enhance the Data Security of Cloud in Cloud Computing'. M K Mahajan . *VSRD International Journal of Computer Science and Information Technology* 2012. p. .

[Li-Qin Tian ()] L C Li-Qin Tian . *Evaluation of user behavior trust in cloud computing. International Conference*, 2010. IEEE. p. .

[Townsend ()] 'Managing a security program in a cloud computing environment'. M Townsend . *Information Security Curriculum Development Conference*, 2009. ACM. p. .

[Jensen ()] 'On Technical security Issues in Cloud Computing'. J S Jensen . *IEEE page(s) 109-116. International Conference on Cloud Computing*, 2009. IEEE. p. .

[Meiko Jensen ()] 'On Technical security Issues in Cloud Computing'. J S Meiko Jensen . *International Conference on Cloud Computing*, 2009. IEEE. p. .

[Sabahi ()] F Sabahi . *cloud computing security threats and responses. 3rd International Conference on*, 2011.

[Raj ()] 'Security on BCCP through AES Encryption Technique'. N S Raj . *International Journal of Engineering Science & Advanced Technology* 2012.

[Mohammed Abdullatif Alzain ()] 'Using Multi Shares for Ensuring Privacy in Database-as-a-Service'. E P Mohammed Abdullatif Alzain . *44th Hawaii International Conference on System Sciences*, 2011. ACM. p. .