IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-2 E-ISSN: 2347-2693

Performance Analysis of Encryption Algorithm in Cloud Computing

Shivlal Mewada[1*], Arti Sharivastava[2],Pradeep Sharma[3], S.S. Gautam[4] and N Purohit[5]

[1*,4] *Department of Computer Science, MGCGV, Chitrakoot, Satna - India*
[2,3] *Department of Computer Science, Govt. Holkar Science College Indore-India*
[5] *Dept of Electronic Communication, Indian Institute of Information Technology, Allahabad- India*

www.ijcseonline.org

Received: Jan /09/2015 Revised: Feb/08/2015 Accepted: Feb/14/2015 Published: Feb/28/ 2015

Abstract—Security is the most important factor in cloud computing for ensuring client data is placed on secure mode in the cloud. Cloud computing is a flexible, cost-effective and proven delivery platform for providing business. Main goal of cloud computing is to provide easily scalable access to computing resources to improve organization performance. In this research paper we have discussed the problem of data security in cloud and show performance analysis to enhance security in terms of encryption algorithm and also explain an overview of cloud and security issues.

Keyword— Cloud Computing, Security Algorithm, AES, DES, Blowfish and RSA.

I. INTRODUCTION

Cloud computing is the concept of using remote service through network using various resources. In cloud computing user can pay on the basis of resources usage as timely basis .In general term we can define it is a technology that provide hosting service over internet it is continuously developed and there are several major cloud providers such as Amazon, Google, Microsoft, Yahoo etc.
Cloud computing is generally divided in to three segments are: "Application", "Storage" and "connectivity" and each segment is used to service as a different service for a different purpose to use in different business.The concept of cloud computing is linked closely with those of service model :

- **IaaS (Infrastructure as-a-services):** It basically deals by providers to provide feature on demand utility.
- **PaaS (Platform as-a-services):** It is used by developer for creating new application.
- **SaaS (software as-a service):** It is provide application as a service on internet.

II. TYPE OF CLOUD

In cloud computing is categorized in four categories

- **Private cloud:** In private cloud data is managed properly within organization only without the limit of network bandwidth .It is some time called internal cloud eg.S3 (simple storage service), EC2 (Elastic Cloud Computing).
- **Public cloud :** This is only one of which cloud service are being available to user via a service provide over the internet it provide service on a pay – per-usage model eg. Google Apps Engine, Blue cloud by IBM.
- **Community cloud:** This type of cloud is basically managed by group of organization that have common objective eg. Security polices etc.
- **Hybrid Cloud:** Hybrid cloud is a combination of private and public cloud means a vendor has a private cloud and form a partnership with a public cloud provider.

III. PROBLEM FORMULATION

Due to constantly increase in the popularity of cloud computing security of cloud become main and top issue of cloud computing such kind of issue become more significant when user want to move critical application and sensitive data to public cloud and shared cloud environment .generally security refer to confidentiality ,integrity and availability .Confidentiality refer who is owner of encryption key .Integrity refer that no common policy exist for approved data exchange the industry has various protocol use to push different jobs. The most problematic issue is data availability some time data is not available on demand of client in that case we can say that security becomes mandatory field in this area.

In cloud computing security can provide in two ways which are:

- Security is provided by service provider.
- Security is provided by the client.

That specifies in cloud computing we can implement security by using two ends either at client end or service provider end total depend on client latest requirement. In this research paper we have discussed the problem of data

Corresponding Author: *Shivlal Mewada,*
Department of Computer Science, MGCGV, Chitrakoot, Satna – India
Email ID: shiv.mewada@gmail.com

security in cloud computing and analysis to enhance security in terms of digital signature and encryption algorithm an also explain an overview of cloud computing and security issues.

The storage security and data security is must to store, manage ,share , analyze and utilize the substantial amount of data residing on cloud should be secure ,authenticated and encrypted so that three level of security can be provided To access cloud based web application that will try to eliminate the concern regarding data privacy segregation . we have analyzed different encryption algorithm such as AES,RSA,DES and Blowfish to ensure security of data in cloud computing .

IV. METHODLOGY

In cloud computing there are various encryption algorithm are used .Encryption algorithm convert the data in to scrambled form by using "the key" and only used have the key to decrypt data .Encryption algorithm is divided in three types :One way trap door: It is one way to encrypt that is not intended to be decrypt .

Symmetric key algorithm: In symmetric key algorithm only one key is used to encrypt and decrypt the message.

Asymmetric key algorithm: In asymmetric key algorithm two keys are used one key(public key)for encryption and other one key (private key) for decryption .

A. Symmetric key algorithm :

DES(data encryption standard): The common UNIX utility ,DES was released to the public in 1970.It is a strong symmetric key encryption algorithm developed by IBM. In 1998 it is replaced by AES.

AES (Advanced encryption standard): It is a strong symmetric key encryption algorithm developed by NIST .it uses 10,12,or 14 rounds each of ciphers has a 128-bit block size with the key size of 128,192 and 256 bits respectively. It ensure that the hash code is encrypted in highly secure manner its algorithm step are follows:

a) Expansion of key
b) Start your preliminary round (initial round)
c) Addition of round key (add round key)
d) Rounds
e) Sub bytes
f) Shift row
g) Mix column
h) Add round key
i) Final round
j) Sub bytes
k) Shift row
l) Add round key.

Blowfish: It is a strong symmetric key encryption algorithm developed by Bruce Schneider in 1993 . The key size of algorithm is different like Blowfish algorithm is 128-448 bits the key size of Blowfish is greater than AES.

B. Asymmetric Key Algorithm:

RSA(RonRivest,Adi Shamir and Lenard Adleman)

It is a strong asymmetric key encryption algorithm created by RonRivest,Adi Shamir and Lenard Adleman in 1978.It is used for public key cryptography. In this two public/private keys are used for encryption/decryption. RSA is not normally a standalone encryption method .It is commonly used conjunction with DES or some other secret key.

DESede:- It is a DES based algorithm in this algorithm encryption is performs in some step:

1. Data is encrypted using DES algorithm and first encryption is done using first sub key.
2. In second step again done encryption using different sub key that called second time encryption.
3. In third step again select sub key (different way as I and II) for encryption.

That means in this technique three time done encryption for security purpose.

V. ANALYSIS OF ENCRYPTION ALGORITHM

In this paper we are analysis encryption algorithm in term speedup and mean time and buffer size in different input. First we define meantime, speed up and buffer size.

1. Meantime is difference between starting and ending time of encryption taken by particular algorithm. If size of data is increase then time taken by encryption is also increase.
2. 2. Speed UP is a difference between mean time cloud and local system. If size of data is increase then speed up may be decrease.

In cloud environment to compare the symmetric key algorithm ,the users implement the application for deploying them on the cloud software environment provider supplies the developer s with programming level environment with well define set of APIs one example is Google Apps Engine ,it provides a runtime environment s and set of APIs. for interaction with Google ' runtime application are run on" sand box ed" environment.

Google APP is free up to certain level of consumed resources , charge applied for additional storage and band width [Rajkumar Buya and Vijeyta Devi] experimental evolution is done on eclipse –SDK and Google App Engine the evolution is done for different input size .10 KB,13 KB,39 KB and 56 KB. For security purpose we used four algorithm AES,DES, BLOWFISH and DESede. Using java on eclipse the algorithm are run local as well as Google app

engine . Here we compare speed-up ratio and Mean time are used to select highest security algorithm .

Table1 (a) Comparison of mean processing time of the algorithm on local system as well as on cloud network . Time is calculated in milliseconds.

Input	AES	AES Cloud	DES	DES Cloud	BLOWFISH	BLOWFISH Cloud	DESede	DESede Cloud
10KB	11.5	1.5	7.5	2	4	2	12	4.5
13 KB	14.7	2	10	2.5	4.7	2	15.5	5.25
39 KB	21	3	3.15	6.5	8.25	2.75	47.25	10.25
56 KB	24.5	3.75	50.25	9.25	15.7	3	70.5	14.5

Table (b) Comparison of local system mean time algorithm with different input only cloud environment

Input	AES Cloud	DES Cloud	BLOWFISH Cloud	DES Cloud	DESede Cloud
10KB	1.5	2	2	2	4.5
13 KB	2	2.5	2	2.5	5.25
39 KB	3	6.5	2.75	6.5	10.25
56 KB	3.75	9.25	3	9.25	14.5

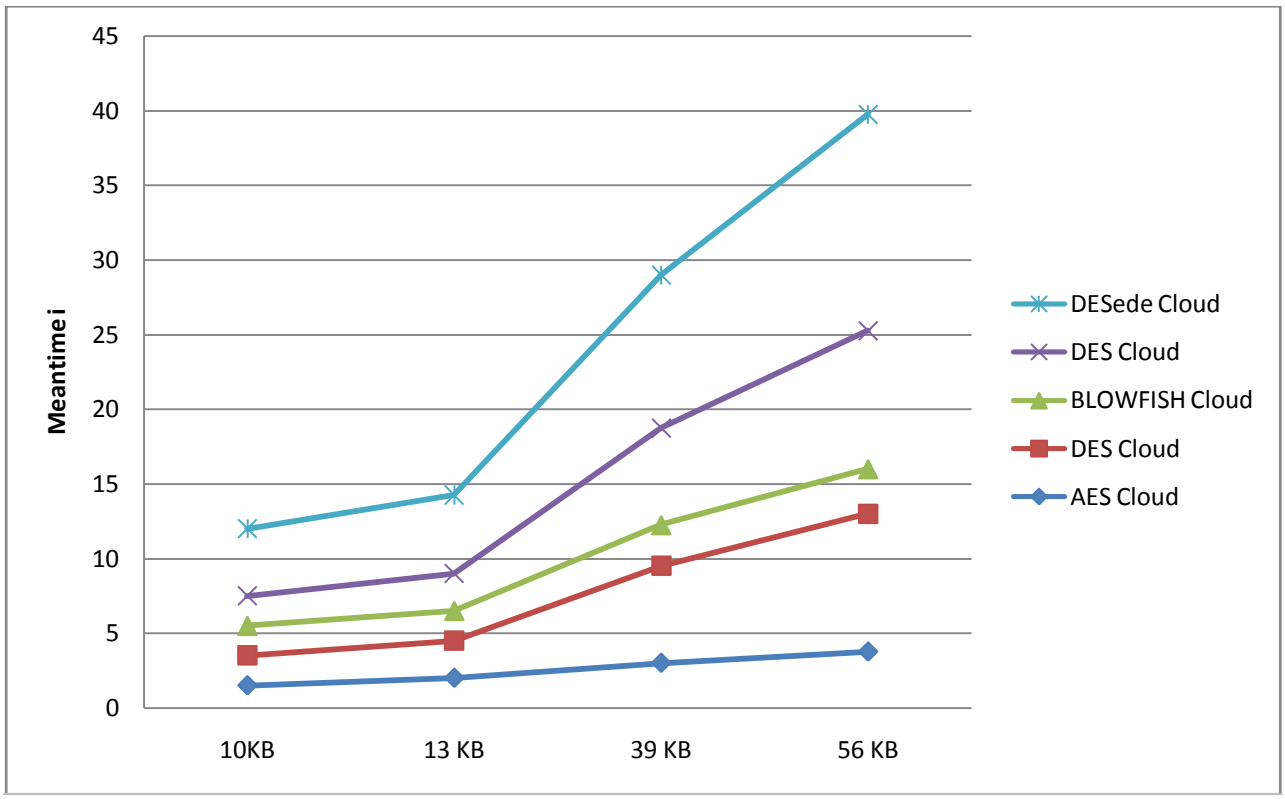

Figure 1:show analysis of mean time for cloud algorithm

Table 3 Analysis speed-up ratio of the algorithm

Input	AES	DES	BLOWFISH	DESede
10KB	7.6	3.62	2	2.6
13 KB	7.2	4	2.3	2.9
39 KB	7	4.8	3	4.6
56 KB	6.6	5.43	5.25	4.8

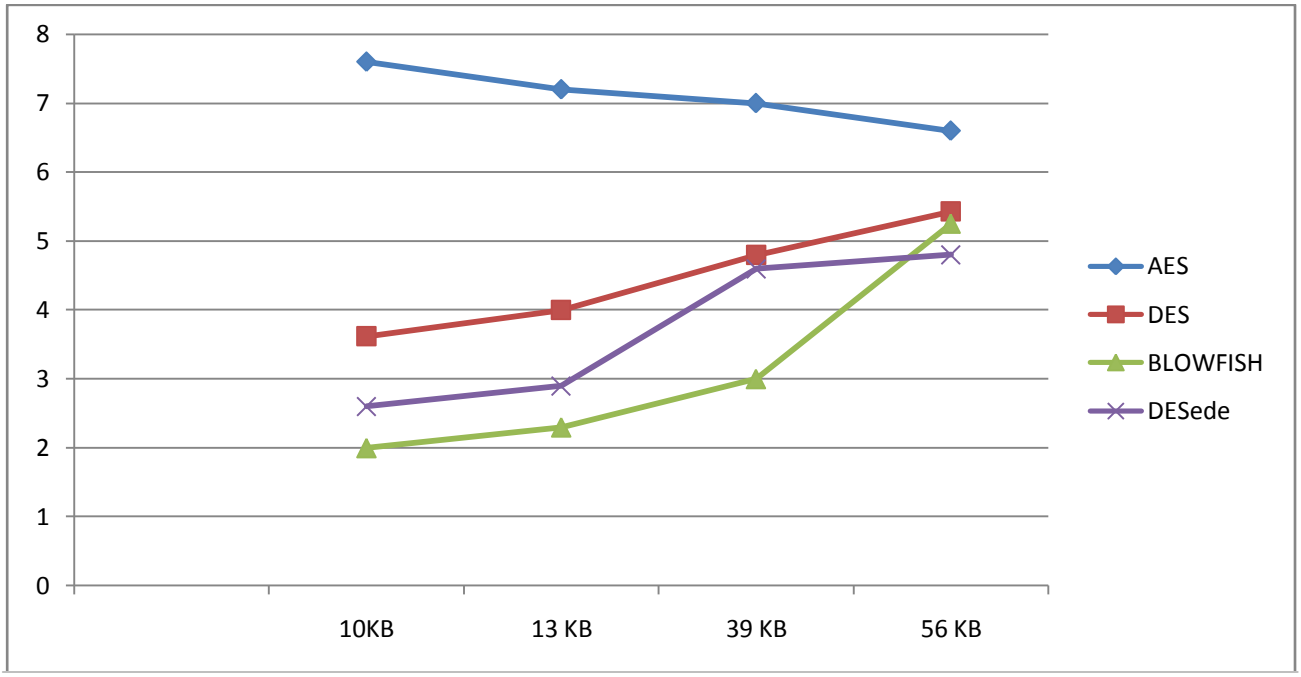

Figure 2: Analysis of speed-up ratio

Given table and chart show performance of algorithm in the basis of the table and graph I observed among all the algorithm DESede symmetric encryption algorithm is average most time consuming and AES symmetric algorithm is less time consuming and Belowfish is least time consuming algorithm and If I see speed-up graph then observation result is AES is highest speed-up in comparison to others.

PERFORMANCE ANALYSIS OF ASYMMETRIC ALGORITHM AND SYMMETRIC ALGORITHM:

In other way analysis on symmetric and asymmetric algorithm in term of buffer size

Table 4: analysis on Buffer size with different algorithm

S.No.	Algorithm	Size	Encryption time in sec.	Decryption time in sec.	Buffer size
1 (Fig-4)	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2 (Fig-4)	DES	*118*	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188

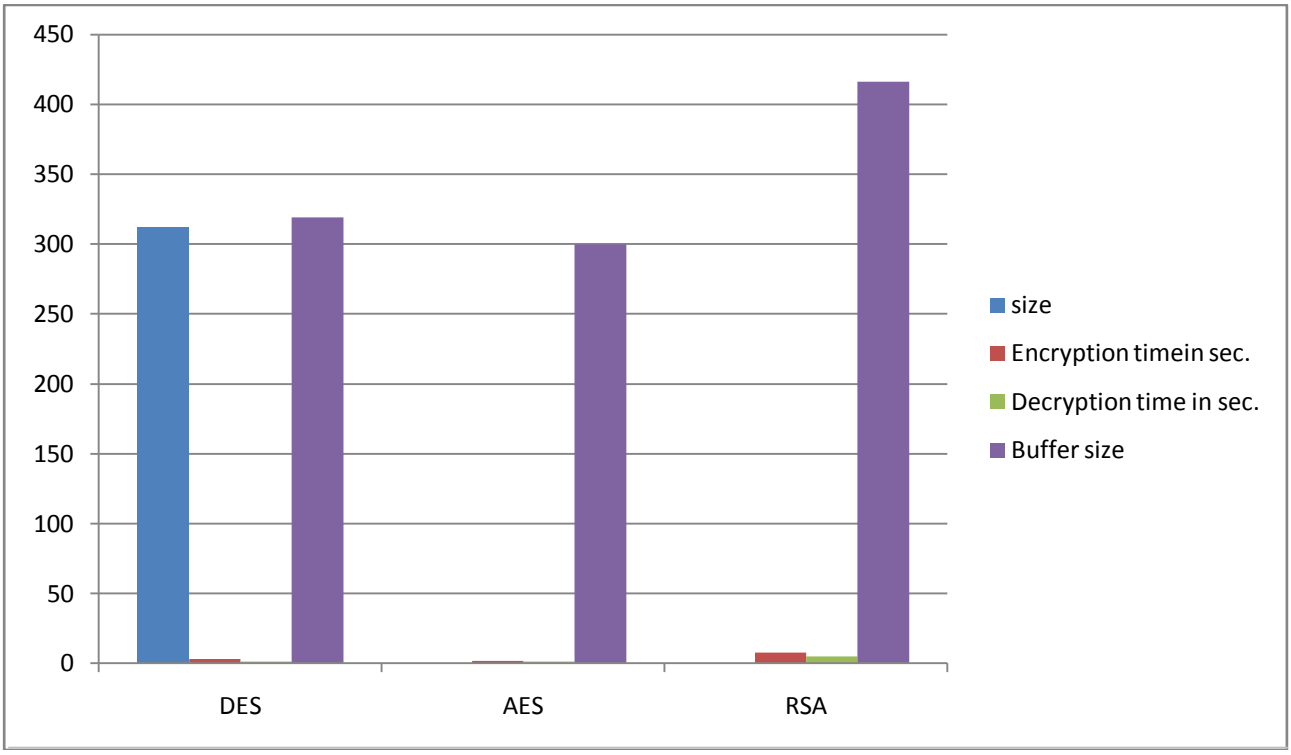

Figure : 4(a):An analysis of algorithm in term of buffer size

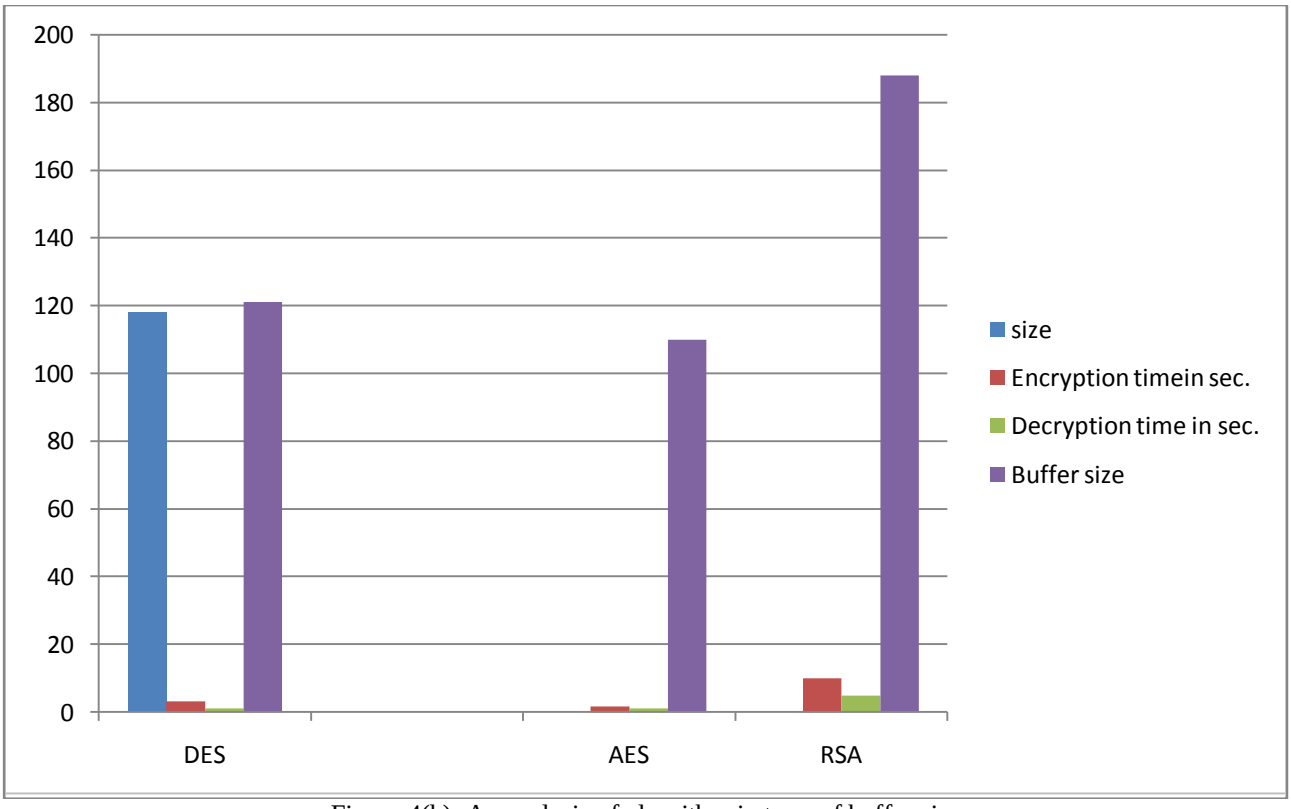

Figure 4(b): An analysis of algorithm in term of buffer size

VI. RESULT

Form tabular result and graph result, the following observation can be made ,using eclipse run variable input size on local as well as on Google App engine. above all algorithm DESede an symmetric encryption algorithm is average most time consuming and below fish is least time consuming .AES – a symmetric encryption algorithm ,the speed up ratio fall sharply with increase in input size .AES algorithm has the highest speed up ratio and then DES.
In 4(a)&(b) Figure show DES is less buffer size and encryption and decryption time in comparison to AES and RSA ,RSA taken more buffer size and encryption and decryption time incomparision to AES and DES. So the following result is draw if we compare among algorithm in term of buffer size the we prefer AES algorithm.

VII. CONCLUSION

The strength of cloud computing is the ability to manage risks in particular to security issues. .In this research paper we have analyzed encryption algorithm and conclude that when you are interested in performance of algorithm then you can prefer BLOWFISH,AES,DES.
If you are interested for the security of data then you can prefer AES.AES algorithm is also good in buffer size.

VIII. FUTURE WORK

In future we will extend our research by providing algorithm implementation and during implementation we also give an option to user to select encryption algorithm according his/her requirement either encrypt or decrypt data on cloud and provide new concept to enhance security in cloud computing.

IX. REFERENCES

[1]. Er. Rimmy Chuchra ,"data security in cloud computing ",International Journal of Societal Application of computer science, Volume -01, Issue -1,Page N0 (1-5),1 Nov 2012.

[2]. Rajkumar Buya and Chee Yeo and Shrikumar," Cloud computing and emerging IT Platform:vision,hype and reality for delivery computing as the 5th utility", Future generation computer system 2009,Page No.(1-15),21 November 2008.

[3]. Bhushan Lalsahu and RajeshTiwari ,"A Comprehensive study on cloud computing" , International Journal of Advanced Research in Computer Science and Software Engineering ",Vol ume-2,Issue -9, Page No.(33-36),September 2012,ISSN 2277.

[4]. M.Vijayapriya ,"Security algorithm incloudcomputing:overview", International Journal of Computer Science and Software Engineering Technology ,Volume-4, Issue-4 ,Page No.(1209-1211),09 September 2013.

[5]. Keiko Hashizume and David G Rosago and Eduardo Fernandez ,"an analysis of security issue for cloud computing " , A Springer Open Journal of Internet Services and Applications, Volume No-4, Issue -5, Page No(22-26),27 February 2013.

[6]. Rashmi and Dr.GSahoo and Dr. S.Mehfuz, " Securing software as a service model of cloud computing issue and solution, "International Journal of Cloud Computing Services and Architecture ",Volume -3,Page No(1-11), Issue -2 ,Augest 2013.

[7]. Shivlal Mewada and Umesh kumar Singh and Pradeep Sharma, "Security Based for Cloud Computing","International Journal of Computer Network and Wireless Communication" ,Volume -1,Issue -1,Page No (13-17),1december 2011.

[8]. Mandieep Kaur and Manish Mahajan ," International Journal of Communication and Computer Technologies ", Volume -1,Issue-3, Page No.(56-59), January 2013.

[9]. Divya Rastogi and Nikunj Kumar," Study of Security Issue in layer in Cloud Computing ", International Journal Of Research Review In Engineering Science & Technology,Volume -2,Issue -2,Page No(30-33),June 2013.

[10]. Parsi kalpna and Sudha Singaraju,"Data Security in Cloud Computing Using RSA Algorithm", International Journal of Research in Computing communication Technologies , Volume- 1 ,Issue -4,Page No(143-146),4 sep2012.

[11]. Debajyoti and Mukhopadhyay and GiteshSonawane and Parth Sarthi Gupta,"Enhanced Security for cloud storage using file encryption", International Journal Of Research Review In Information Tchnology ,Department of IT ,Volume -2,Issue -1Page No(11-15), 2013.

[12]. NehaTirthaniGenesenr."Data security in cloud arxhitecture based on Diffie Hellman and Elliptical curve cryptography", Volume- 1,Issue-1,Page No [1-4].

[13]. B.N. singh ,"Cloud Development Model", example [online available]20 may 2014.

[14]. Kai hwag and Deyili," Trusted Cloud Computing with Secure Resources and Data coloring",IEEE ,Volume-14,Issue-5,Page No(14-22),2010.

[15]. V.D cunsolo and S.distenfo," Achieving information security in network computing system",IEEE,Page No (77,-80),Dec 2009

[16]. Dr.Sunil Batra and Anju chibel ,"Preliminary Analysis of Cloud Computing Vulnerabilities", Journal of Engineering computer and Applied science ,Volume- 2 ,Issue -5,Page No(49-51),May 2013.

[17]. Venkata Krishna kumar and S padma priya ," A survy of cloud computing security threat and vulnerabilities ",International journal of innovative research in electrical, electronics, instrumentation and control engineering ,Volume- 2 ,Issue -1,Paga No(622-625),January 2014.

[18]. A.T. valte and T.J.velte and R.C.," Cloud Computing a Practical Approach " Tata McGraw -Hill,First(I st) Edition,USA 2009.

[19]. Farzadsabhi,"Cloud Computing Threat and Responses" ,IEEE, Page No(245-249) ,27-29 may-2011

[20]. Ros and jacobo," Security in Cloud the Threat of co exits with an unkown tenant on a public environment" , Page No(), Royal Holloway ,University of London

[21]. Gurpreet Kaur and Manish Mahajan, "Evolution and Comparison of Symmetric Key algorithms", International Journal of Science ,Engineering and Technology Research, Volume-2,Issue -10, Page No(1960-1962),October 2013,ISSN 2278-7798.

[22]. Vijeyta Devi and Vadlamani Nagalakshmi, "A Prospective Approach on Security with RSA algorithm and cloud sql in cloud computing", International Journal of Computer Science and Engineering ,Volume n-2,Issue -2 ,Page No(35-44),May 2013.

[23]. Uma Somani ,"Implementation Digital Signature with RSA Encryption algorithm to enhance the data security of cloud in cloud computing",2010.

[24]. Ms. Disha H. Parekh and Dr. R. Sridaran," An Analysis of Security Challenges in Cloud Computing", Volume – 4,Issue-1, page No.(30-44),2013.

[25]. Navneet Sharma and Vijay Singh Rathore, " Different Data Encryption Methods Used in Secure Auto Teller Machine Transactions", Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-4, Page No.(176-177) April 2012.

[26]. Madhu Chauhan and Riidhei Malhotra and Mukul Pathak and Uday Pratap,"DIFFERENT ASPECTS OF CLOUD SECURITY " , International Journal of Engineering Research and Applications, Volume -2 ,Issues-2,Page No.(864- 870) , Mar-Apr 2012.