Three Level Cloud Computing Security Model

Pooja Sharma
Student
Masters of Technology
Galgotias College of Engineering and Technology

Rajkumar Singh Rathore
Assistant Professor
Department of Computer Science & Engineering
Galgotias College of Engineering & Technology

ABSTRACT

Cloud Computing is the next generation technology that describes the development of many existing technologies and approaches to computing into something different. Cloud enhances agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing[1]. Cloud Computing has the potential to change the nature of Information and Communication Technology (ICT) provision in the public service and significantly reduce costs[1]. It is a key element of strategic future of ICT in this sector. Cloud Computing services are delivered by any third party provider who has its own infrastructure. As cloud is a collection of super computers which are spread all over the world, hence authorization and authentication are extremely necessary. This paper proposes a methodology to over come the security threats that can take place on three levels i.e login authentication, network security and Storage Security. We have built an Email system to provide security on all three levels. Firstly, user authentication is done so that an unauthorized user cannot tamper the data of authorized user. Secondly, when the user wants to check its inbox, then he is supposed to enter the passcode i.e Storage Security via RC4 is done. Thirdly, while sending a mail to someone through network is done with the help of AES (Advanced Encryption Standard). Hence, the integrity and confidentiality of data saved in inbox or mailed to another user is ensured by not only encrypting but also providing access to data only on successful authentication.

General Terms

Cloud Computing, Security, Security Issues

Keywords

AES(Advanced Encryption Standard),RC4.

1. INTRODUCTION

Scott McNealy, former CEO of Sun Microsystems said that ,"We believe we are moving out of the Ice Age ,the Iron Age, the Industrial Age, the Information Age, to the Participation Age. You are participating on the Internet, not just viewing stuff. We build the infrastructure that goes in the data center that facilitates the participation Age." Cloud computing is a buzz word. Ex. Obama won the election because of cloud computing. It was the key factor because it used the amazon web services quite effectively to channelize the voters who believe in Obama. He tried to run some application on amazon web services and uses the amazon powers and that channelized the voters who believed in Obama. All voters who didn't come out to vote and were favouring Obama they too voted .That brought a huge amount of victory to Obama .

A recent Forrester reports "Sizing the Cloud" notes: The cloud computing market will rise from $40.7 Billion this year to more than $241 billion in 2020, with year-to-year growth over 20 percent. It was almost as much revenue of apple or more than that. Estimate tremendous growth in IaaS with its market size estimated over to be 80 percent of the global public cloud market.

2. SECURITY REQUIREMENTS

Cloud Computing has three major research areas and those are security, performance and availability. Cloud Computing security is at the top of all three of them. Considering four different service levels such as IaaS, PaaS, SaaS, and physical data center cloud computing is divided into four levels, i.e Infrastructure level/Virtual level, platform service level, application level and physical level respectively[2].

2.1 Physical datacenter

Users: Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed[2].

Security Requirements: Hardware Security, hardware reliability, network protection, legal not abusive use of cloud and network resources protection[3].

Threats: Network attacks, Connection flooding, DDOS, hardware interruption, hardware theft, hardware modification, misuse of infrastructure and natural disaster.

2.2 IaaS/ PaaS

Users: Developer-moderator applies to a person or an organization that deploys software on a cloud infrastructure.

Security Requirements: Access control, application security, data security, Cloud management control security, Secure images, Virtual cloud protection and Communication security[2].

Threats: Programming flaws, Software modification, software interruption (deletion), Impersonation, Session hijacking, Traffic flow analysis, exposure in network, DDOS, Disrupting communications.

2.3 SaaS

User: End Client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use.

Security Requirements: Privacy in multitenant environment, Data protection from exposure (remnants), Access control, Communication protection, Software security, Service availability[1].

Threats: Interception, Modification of data at rest and in transit, Data interruption(deletion),Privacy breach, Session hijacking, Exposure to network[2].

3. SECURITY IMPLEMENTATION ON CLOUD MODEL

3.1 Log Based Authentication

The login records are saved in a separate file known as Log Records. Log Record consist of Username, Password and Date & Time. If an un-authorised user logs in then it can be detected by checking the Log records. Ex: facebook, where login records are saved with the time of logging and the location from where the account is logged in.

3.2 Network Level Security

If an un-authorised user Login by some means ,then it again needs to provide the passcode for performing some action such as deletion, transaction , etc .Example : Similar to OTP(One Time Password) but the passcode remains. Inbox passcode and login password can be different. For Network Security, AES(Advanced Encryption Standard) Algorithm would be used. The AES encryption Technique and OTP has provide solution for secure transfer to the cloud. Network Security is achieved by applying AES Algortihm.

Implementing AES

In 1997, call for AES arrives by NIST(National Institute of Science and Technology)[4]. In August 1998, 15 algorithms were submitted out of which 5 finalist algorithms were selected. On 2nd Oct,2000 Rijndael was chosen as the AES,designed by Joan Daemen and Vincent Rijmen.

AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds[5].

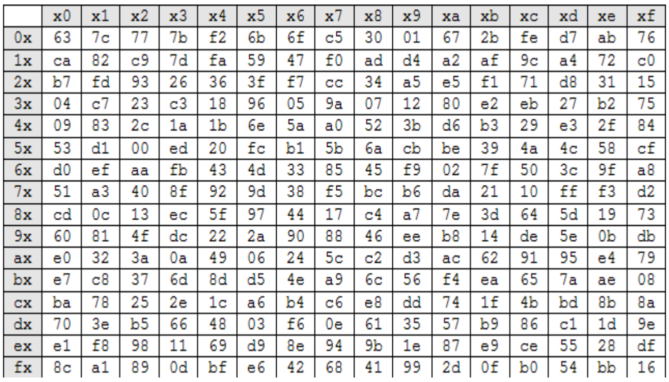
Key size	No. of rounds
128	10
192	12
256	14

Each round consist of 4 layers:

a) Byte Substitution: The first transformation , SubBytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits. We apply S- function of Ai bytes and get Bi byte S-function i.e substitute function. The SubBytes operation involves 16 independent byte-to-byte transformations[6].

$$S(Ai)=Bi$$
$$Ai=(X,Y)$$
$$X=C,\ Y=2\ (hexadecimal\ numbers)$$
$$Ai=(C2)_{16}$$
$$Bi=S(Ai)=S(C2)_{16}=25$$
$$Ai=(C2)_{16}=\{\ 11000010\}$$
$$Bi=25=\{00100101\}$$

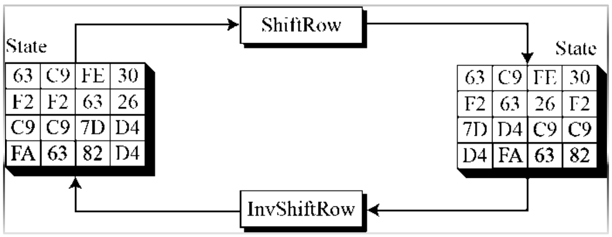
Here each byte is substituted using Substitution Box(S-Box). There are 16 byte-to-byte substitutions and the S-box is majorly constructed by combination of GF(28) arithmetic.



	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. 1: Substitution Box

b) Shift Rows: It is a transposition step where each row of the state is shifted simply by using permutation[5]. Each row is shifted cyclically at a certain number of times.



63	C9	FE	30
F2	F2	63	26
C9	C9	7D	D4
FA	63	82	D4

63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C9
D4	FA	63	82

Fig. 2: Shift Row Transformation Step

c) Mix Columns: It is an interbyte transformation that changes the bits inside a byte. We have diffusion on algorithm at bit level means one bit change in input provides extremely different output. It is simply the matrix multiplication where each value of the column is multiplied by every row value. Results are XORed together[5]. Entire output of mix column get affected if one single bit is flipped in input.

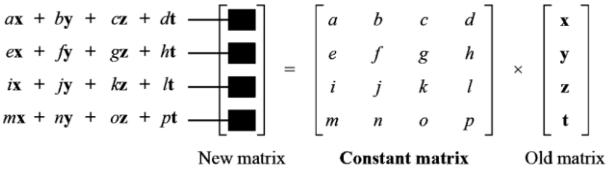


Fig. 3: Mix Column Transformation step

d) Add Round Key: Each byte of the state is combined with the round key. The round key is derived from the main key or cipher key using a key schedule, where each subkey size is same as that of state. AddRoundKey transformation is the inverse of itself[6].

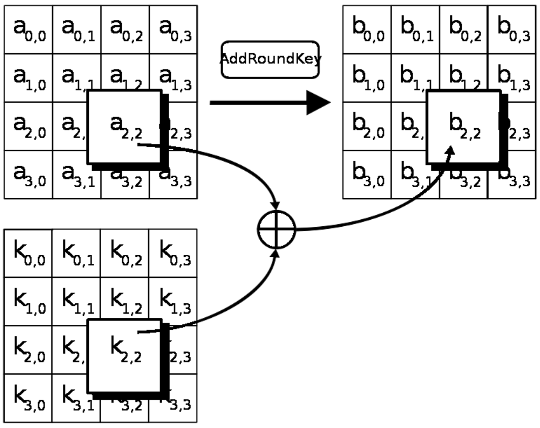


Fig. 4: AddRoundKey Operation of AES

3.3 Storage Level Security

The storage level of cloud computing security model follows the Algorithm RC4[7]. RC4 is a stream cipher symmetric key encryption algorithm which is based on the use of random permutations and generate pseudo random stream of bits. In this a single algorithm is used for encryption and decryption as data stream is simply XORed with the generated key sequence[8]. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. It is a 256 bit array(S[256]) containing a permutation of 256 bytes. While initializing the state table there are two 256 bytes array are taken: S-Box and K- box. S-Box contains linear numbers which are S_0=0,S_1=1,S_2=2,…S_{255} =255 and K-Box includes key which is to be used in repetition to fill the array. The key setup and key generation is performed for every new key to generate a unique key. In key set up phase S-Box is modified using pseudo random codes. It uses two counter i and j[9].

Key Setup phase:

```
j=0
for i from 0 to 255
j = ( j + S[i] + K[i] ) mode 256
swap ( S[i] , S[j] )
end for
```

Pseudo Random Key Generation Phase:

```
i = 0
j = 0
ptlen = length( plaintext )
while ( ptlen>0 )
i = ( i+1) mod 256
j = ( j+ S[i] ) mod 256
swap ( S[i], S[j] )
key = S [ ( S[i] + S[j] ) mod 256 ]
output key
ptlen = ptlen-1
end while
```

Once the pseudo random key is generated then plain text is XORed with it to generate cipher text.

4. WHY AES AND RC4?

The requirement of our project was to provide as better security as possible. AES has been proved as the most successful security algorithm. AES by now is the most important symmetric algorithm in the world. More than 50% products that required high level security uses AES. AES has been used by web browsers, VLANs, Wi-Fi connections and many million applications. NSA (National Security Agency) allows AES for classified data upto TOP SECRET with 192 or 256 bit key. NSA has smart cryptographers employed. Big intelligence says that they trust AES. There are no serious weak keys in AES. AES supports any block sizes and key sizes that are multiples of 32(greater that 128 bits).AES is more secure than DES due to large size key. Huge number of tests have failed to do statistical analysis of the cipher text. AES structure has good potential which is benefitted from instruction level parallelism. Performance of AES is good in both hardware and software platforms under different environment. It includes 8-bit and 64-bit platform and DSPs. IT not only assures security but it also improves the performance in a variety of settings such as smartcards, hardware implementations etc. AES is federal information processing standard and there are currently no known non-brute-force direct attacks against AES.

	DES	**AES**
Date	1976	1999
Block Size	64	128
Key length	56	128,192,256
No. of Rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, Diffusion	Confusion, diffusion
Design	Open	Open
Design Rationale	Closed	Open
Selection process	Secret	Secret but accept open public comment
Source	IBM enhanced by NSA	Independent cryptographers

Table 1: Comparison between AES and DES

RC4 is a stream ciphers, so it works on only a few bits at a time they have relatively low memory requirements (and therefore cheaper to implement in limited scenarios such as embedded devices, firmware, and esp. hardware)[8]. RC4 is very fast. Faster execution means less computation needs and therefore lower hardware requirements, while RSA is very slow in execution[7]. As we know, RC4 is a stream cipher and it is widely used technique because block ciphers were found to have issues (like BEAST and LUCKY 13). RSA is asymmetric key cryptographic technique. It needs sharing of public key from both communicating parties,so not recommended in public environment like internet users.

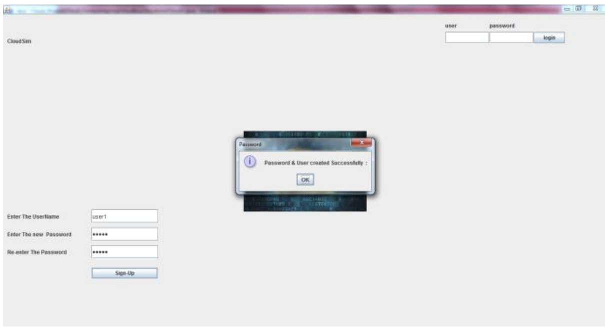
Parameters	**RSA**	**RC4**
Speed	Less faster	1000 times faster than RSA
Applications	Highly confidential Data	Personal files, Wireless and TCP/IP transmission.
Complexity	Highly complex	Simple
Security	Highly Secure	Moderately Secure

Table 2: Comparison between RSA and RC4

5. RESULTS AND DISCUSSION

In this paper a simple email system is developed which focuses on the security provided at different levels.The steps followed by our work are as follows:

a) The user registers itself by providing its username and password as shown in fig. 5.

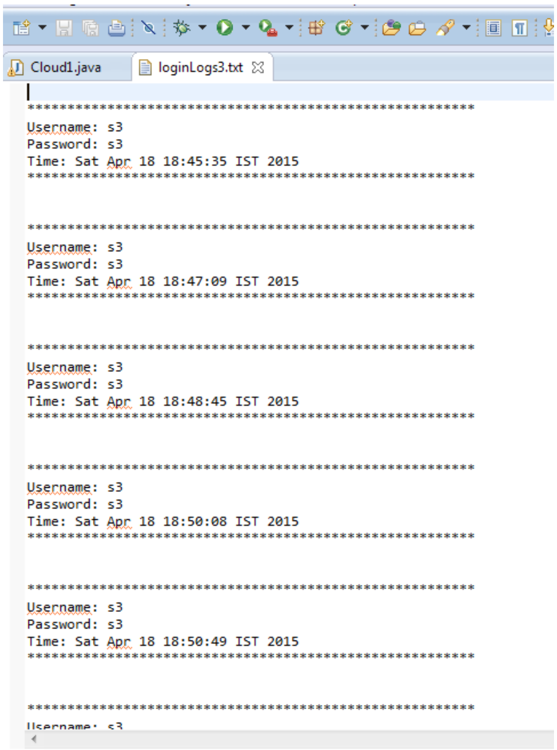


Password & User created Successfully :

Enter The UserName: user1
Enter The new Password: *****
Re-enter The Password: *****

Fig. 5: User Registration and Login Page

b) User logins by correctly providing its username and password. Every time the user login, its Login details are saved in a separate file called as log Records. If an unauthorized user logins at an unexpected time then it can be easily checked by checking the login details. Hence all the information related to login can be retrieved. Login Records includes the username, password, Date and Time of Login as shown below in fig. 6.



```
*********************************************************
Username: s3
Password: s3
Time: Sat Apr 18 18:45:35 IST 2015
*********************************************************


*********************************************************
Username: s3
Password: s3
Time: Sat Apr 18 18:47:09 IST 2015
*********************************************************


*********************************************************
Username: s3
Password: s3
Time: Sat Apr 18 18:48:45 IST 2015
*********************************************************


*********************************************************
Username: s3
Password: s3
Time: Sat Apr 18 18:50:08 IST 2015
*********************************************************


*********************************************************
Username: s3
Password: s3
Time: Sat Apr 18 18:50:49 IST 2015
*********************************************************


*********************************************************
Username: s3
```

Fig. 6: Login Records

c) After the user logins successfully, he is redirected to new window i.e fig. 7 where he can perform 3 options i.e Change Password, Mail_Box and logout.

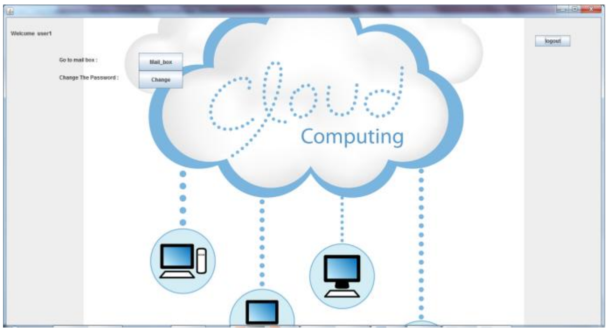
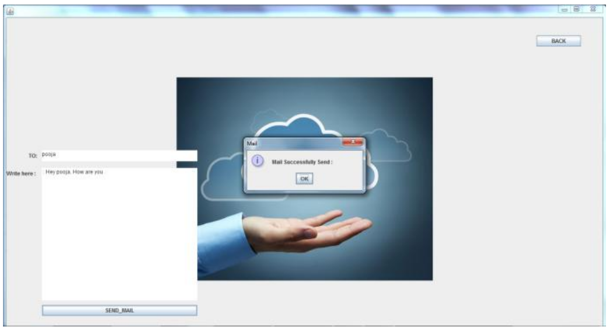


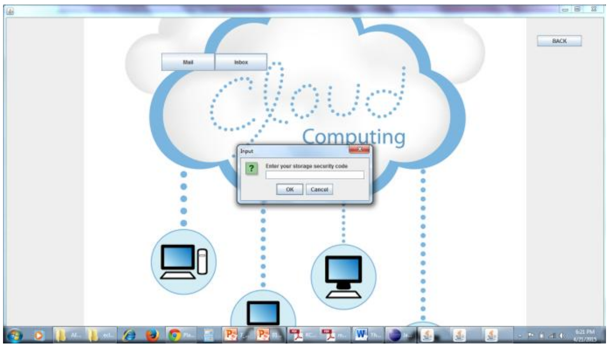
Fig. 7: User Account

d) On clicking the mailbox button , the user will be redirected to new screen i.e fig.9 on which he can select Inbox or Mail. Inbox is a storage where the RC4 is applied and the mails are saved. On clicking mail button, the user will be redirected to another screen as shown below in fig. 8, where he can write its mail and he is supposed to enter the correct user name in its To field.



TO: pooja
Write here : Hey pooja. How are you
Mail Successfully Send :

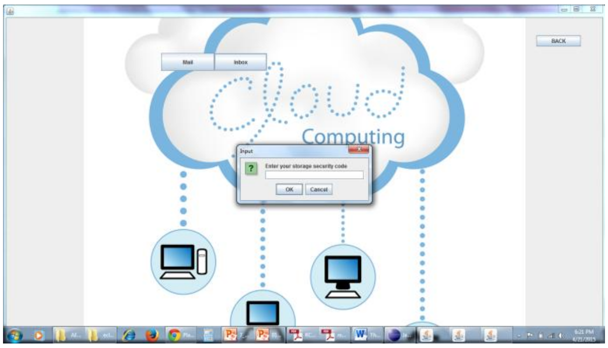
Fig. 8: Send Mail Screen



Enter your storage security code

Fig 9:First time User Inbox Authentication

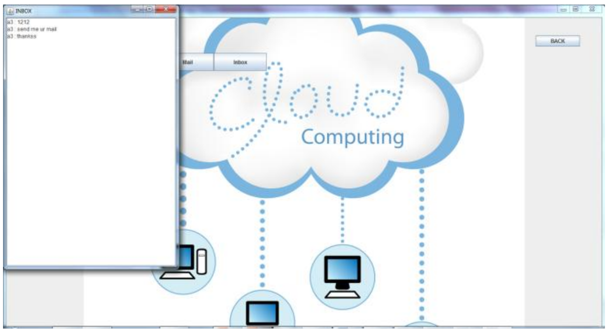
e) To check the mails, one needs to click on the inbox button. The first user will have to generate its first time storage security code as shown in fig. 9. After that, every time the user open its inbox, he is supposed to enter its passcode that was provided by him at the very first time he opened the inbox i.e the storage security code provided by him as shown below in fig. 10.


Input

Enter your storage security code

Fig. 10: Providing storage security code to check the mails

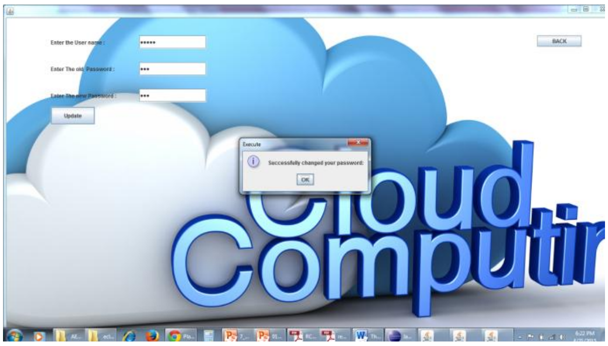
f) A new window is opened after providing the correct security code and hence the authenticated user can check its mails. After successful login, the inbox is shown in fig. 11


INBOX

a3 : 1212
a3 : send me ur mail
a3 : thankss

Fig. 11: Inbox

g) One can also change its password by clicking on the Change password button which is provided above in step c. The change password screen is shown below in fig.12.


Enter the User name : *****

Enter The old Password : ***

Enter The new Password : ***

Execute

Successfully changed your password:

Fig. 12: Change Password Page

6. REFERENCES

[1] Jaydip Sen, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, Security and Privacy Issues in Cloud Computing.

[2] Dimitrios Zissis∗, Dimitrios Lekkas, Addressing cloud computing security issues, journal homepage: www.elsevier.com/locate/fgcs, Future Generation Computer Systems

[3] Rajkumar Chalse, Ashwin Selokar 2013 5th *International Conference on Computational Intelligence and Communication Networks*, A New Technique of Data Integrity for Analysis of the Cloud Computing Security.

[4] R. H. Sakr1, F. Omara2, O. Nomir3, May-June 2014, *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* An Optimized Technique for Secure Data Over Cloud OS.

[5] Abha Sachdev, Mohit Bhansali, April 2013,*International Journal of Computer Applications* ,Enhancing Cloud Computing Security using AES Algorithm.

[6] Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal, Enhanced Security for Cloud Storage using File Encryption.

[7] Smriti*, Dr. Deepak Arora**,Jul-Aug 2013, *International Journal of Engineering Research and Applications*, Ensuring Data Security for Secure Cloud Hybrid Framework.

[8] Bhagyashri C. Allagi , Dr. R. B. Kulkarni, Shashikant Hippargi,November 2013,*International Journal of Advanced Research in Computer Science and Software Engineering*, Cloud Computing for Media Storage and Performance Analysis.

[9] Prof Swarnalata Bollavarapu, Bharat Gupta, March 2014, *International Journal of Advanced Research in Computer Science and Software Engineering*, Data Security in Cloud Computing.

[10] Vijay. G.R, A.Rama Mohan Reddy,*International Journal of Soft Computing and Engineering (IJSCE)*,Data Security in Cloud based on Trusted Computing Environment.

[11] T. Saravanan, 1 2G. Saritha and 3R. Udayakumar, 2014, *Middle-East Journal of Scientific Research*, Secure and Trustworhty Data Storage in Cloud Computing.

[12] Uma Naik1, V. C. Kotak2, *Feb. 2014 OSR Journal of Electronics and Communication Engineering (IOSR-JECE)*,Security Issues with Implementation of RSA and Proposed Dual Security Algorithm for Cloud Computing.

[13] Zhang Xin, Lai Song-qing, Liu Nai-wen, 2012 *INTERNATIONAL SYMPOSIUM ON INFORMATION TECHNOLOGY IN MEDICINE AND EDUCATION*, Research on Cloud Computing Data Security Model Based on Multi-dimension.

[14] Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1, *Journal of Internet Services and Applications 2013*, An analysis of security issues for cloud computing.