ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

RC4 and DES based Cloud Computing Data Security and Comparison

Sheetal Mahalle [1],Ranjeet Jaiswal [2]

Computer Science Department, TIT Bhopal,India[1]

Professor, Computer Science Department,TIT Bhopal,India[2]

Abstract: Cloud computing is wider used now a days because of on demand use, flexibility, virtualization, easy portability etc. features. The features are useful in all areas and widely used by different customers like Social websites, E-Commerce, Education and heavy data warehouse system. As huge data can be shared and distributed with the requested resources very vastly so the need of security arises in the cloud computing workflow. So for securing the cloud data as a trusted party developed a secure framework with the help of RC4 and DES capability. User control is the primary security concern provided in our paper. Distributed virtualizations on demand advantage are also included with the attack detection mechanism, so the method will provide better security in self-loop user also.

Keywords : Cloud Computing, Virtualization, Security, RC4, DES.

I. INTRODUCTION

The resources can be considered as the dynamic pool which is the main advantage of the cloud computing [1][2][3]. From the piece of standard enrolling the good circumstances of conveyed processing are: status, lower area cost, device independency, territory independency, and adaptability [5]. Yet the security concerns are the noteworthy key points later on dispersed processing period. There are a couple security majors are shown in [6], [7],[9],[10],[5].Virtualization, first class figuring are also the more noticeable office parts of circulated registering. Regardless to achieve the execution on the parallel structure and keeping up the dependability is amazing [11]. In every one of these works, unprecedented attempts are made to blueprint courses of action that meet distinctive requirements: high arrangement capability, stateless checks, unbounded usage of request and sadness of data, et cetera.

Considering the piece of the verifier in the model, all the arrangements brought before fall into two classes: private auditability and open auditability [5]. Disregarding the way that arranges with private auditability can achieve the arrangements viably, yet it is trying condition if the data is securing covertly [5]. Virtualization is the key eccentricity of dispersed processing by which data conferring is possible between unmistakable machines of virtual vicinity from the server ranch [12]. Virtualization enables the live development [9] of virtual machines (i.e. moving a VM beginning with one host then onto the following without cutting it down) which helps in keeping up the ensured SLA to the cloud buyer besides for conforming load transversely over physical servers in the data centers[12]. It can be utilized as a part of the appreciation of college undertakings also [13].

The fundamental cloud suppliers are Google, Microsoft, Salesforce.com, Vmforce.com and Amazon and so forth.

The distributed computing framework relies on upon the layers for data transportation. The three rule organization layers that include the conveyed figuring building plan in light of which the on interest organization will be provided [14]. According to [14] Software as a Service (SaaS) has changed desktop-based programming applications into web programming things that can be used the world over. A for the most part used application is Salesforce.com, a customer relationship organization (CRM) programming for associating with associations and clients[14]. As showed by [14] Platform as a Service (PaaS) is a space for Cloud Computing Security Management for making and building applications for differing circumstances.
According to Infrastructure as a Service (IaaS) fundamentally incorporates virtualization circumstances as purchased organizations rather than physical[15][16].

II. LITERATURE SURVEY

In 2012, Wentao Liu et al. [14] suggest that the security issue of appropriated processing is vital and it can keep the quick headway of circulated registering. It displays some dispersed processing structures and dismembers disseminated figuring security issue and its technique according to the appropriated registering thoughts and characters. The data assurance and organization availability in disseminated figuring are the key security issue. Single security framework can't deal with the conveyed registering security issue and various ordinary and new developments and systems must be used together for securing the total appropriated processing structure.

In 2013, Nikhilesh Pant et al. [15] present the strategies for cloud allocation and cloud security assessment to research potential security and suitability recommendations in cloud environment. They looks at in unobtrusive component on how an affiliation may proceed for security and pleasantness examination in the midst of the cloud figuring. Their strategy and thoughts point by point in this paper would be useful for affiliations that are incorporated in the cloud choice procedure.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

In 2013, Du meng et al. [16] analyzes dispersed registering data security issues, including tile security of data transmission, stockpiling, security and organization of security. Focus on broad data organization impact cloud security examination, and pointed out that a jump forward in the headway of this dispersed processing, endeavor to distinguish the relating frameworks and whole deal change bearing.

In 2013, Fan Yang et al. [17] suggested that the data security and insurance on cloud is a crucial issue, transforming into the best limit of dispersed processing change. A Trusted Cloud Computing Platfom (TCCP) considering remote affirmation amass a trusted cloud for tenant. The essential portion is fused Trusted Coordinator, taking the spot of inhabitants to affirm center points solely in disseminated registering stage. In any case, when an extensive measure of tenants solicitation centers meanwhile, Trusted Coordinator (TC) maybe can't deal with these requesting quickly .To address this issue, they propose the establishment of security-level for unmistakable applications in TCCPs, which segments Trusted Coordinator into three, each accountable for checking different application kind. The different check approaches, for instance, customer watchword relationship, picture hash affirmation and trusted chain estimation, as demonstrated by particular security levels.

In 2013, Issa M. Khalil et al suggest that the Security issue in circulated registering is shown to be the best hindrance that could subvert the wide benefits of conveyed figuring. The new thoughts that the cloud presents, for instance, multi-residency, makes new challenges to the security bunch. Keeping an eye on these challenges obliges, despite the ability to create and tune the endeavors to set up wellbeing made for diverse structures, proposing new security game plans, models, and traditions to address the novel cloud security challenges. They give broad examination of disseminated registering security that joins gathering of known security risks and the best in class practices in the attempt to adjust these perils. They in like manner give the dependence level inside course of action and give an answer in sign of preventive exercises instead of proactive exercises.

In 2013, Azzedine Benameur et al. [19] prescribe that that the circulated processing standard for broad scale bases and more military and fundamental base structures are moving towards cloud arranges as well. They show an approach to impact the adaptability and on-enthusiasm provisioning contrivances of the cloud to improve quality to availability concerns and normal strikes. Their system uses growing of lightweight virtualized application servers for abundance and confirmation against both application mix-ups and framework based strikes.

In 2013, Liu Xiao-hui et al. [20] prescribe Cloud enrolling gets the chance to be more common to people, and its application field gets the chance to be all the more by and large. They exhibited its change status, and analyzed the security issues. Propelled a couple trains of considered the security, and suggested that trusted disseminated figuring will be an ensuring bearing without limits cloud security investigates[24].

III. PROPOSED METHODS

The framework of cloud computing has been designed using java server pages (JSP) on the Net beans tool. The basic functionality of Java is also being used. The developed entrepreneur server is based on 4 different cloud providers' servers. The resource allocation scheme is different for the different servers and it will depend on the data storage capability. The cloud user can upload the data after registering their details on the cloud environment. This will complete the authentication process and maintain the log file for the user and all the space, time and attack detection mechanism are controlled from this event. Figure 1 working process chart clearly shows this mechanism.

Our proposed approach provides security with two standard encryption mechanisms namely Data Encryption Standard (DES) and Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm. In this approach the registered user first selects the server from the 4 specified above. Space is managed virtually and it will relocate the space as per the demand by the user without any interruption. The data is then uploaded in the selected server as requested by the user and it is then available for the self-use purpose immediately. The data is then available to share to other authentic users in the cloud from any four servers. For the testing case we have restricted the file type to text only so that proper comparison can be provided with the same type of data. If the registered user wants to access the data of other user, it can be accessed on request to the particular user via the cloud service provider. If the user grants the data then only other user can access the data. This is the first speciality of our work. Means our work provides data sharing capability but with the secure data transaction. The user data are restricted for view to the cloud providers so data read permission is not for cloud providers also. This is the second speciality of this work. If the other cloud user agrees to share the data to another cloud user then the data is prepared for sending it to the respected cloud user. The data is prepared with RC4 and DES mechanism and the plaintext is changed to cipher text according to RC4 and DES mechanism both. Then a hash file is send with the data that will automatically render the notification to the service provider if the not designated user will open the file first. As the security is by standard encryption technique it will provide a better and strong against brute force attack. This the third concept added in our framework. Then the recipient can access the data after applying both RC4 and DES encryption standard mechanism. If any other user opens the files the hash tag alerts the mismatch operation to the cloud provider. The keys are random generated so for the same file the keys are different. So tracing it is different.

We have also maintained the efficient virtualization mechanism which will enable the vitalization space according to the requirement. So that the load will be

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

properly distributed. This is the fourth advantage of our work. In this we have adopted 500 KB + file size scheme for this mechanism. Means the space will automatically acquire the space 500 Kb + size of the files which is to be uploaded.

The working algorithm of our methodology is shown below:

Proposed Algorithm

The data queue and the standard encryption algorithms are shown below which is used in file preprocessing.

1) Inputs: Cloud Data set for sharing (CF_1, CF_2…….CF_n).
2) Output: File prepared by the cloud user (FP_1, FP_2 ……..FP_n).
3) do
   The peak request has been selected based on first come first serve basis. The load request can be denoted as (lr_1, lr2……lr_n) from the total request received.
   For the each request received (LR= lr_1, lr_2……lr_n)
   Input: The data bytes have been supplied
   RC4
   Algorithm: RC 4[25]
   Stream cipher symmetric key
   Use two arrays, state and key
4) 256-byte state table.
5) State [256]=[0 .. 255]
6) It has the capability of using keys between 1 and 2048 bits.
7) Key [1..2048] = […….]
   Two phases
   ‰ Key Setup
   f = (f + Si+ Kg) mod 4
   Swapping Siwith Sf
8) Ciphering (XOR)
9) 1. i = (i + 1) mod 4 , and f = (f + Si) mod 4
10) 2. Swaping Si with Sf
11) 3. t = (Si+ Sf) mod 4
12) Random byte St Send data to the client with relevant log file and also maintain a log report for this event.
13) Finish.

Algorithm 2: DES Algorithm for Encryption and Decryption

1) Take plaintext (PT) as 64-bit and handover it to Initial Transposition/Permutation function (IP).
2) Perform Initial Transposition function on acquired PT and produce the acquired text into two equal halves: Plaintext of Left side (say PTL) and a Plaintext of Right side (say PTR).
3) Perform 16 rounds over both these halves via Heart of DES or DES function using 56-bit key on each round. Each round of DES is a feistily cipher.
4) The DES function applies a 48- bit key to the rightmost 32-bits to produce a 32-bit output. We can make all 16 rounds the same by including one swapper to the 16th round and add an extra swapper after that as two swappers cancel the effect of each other. For each round (R'= r'1, r'2…, r'16) do A. Perform Key transformation or Compression permutation by reducing the original 56-bit key to 48-bit key.
5) Expand PTR from 32-bits to 48-bits ensuring bits transposition. This can be done through Expansion P-box. Although the relationship between the input and output can be defined mathematically, DES uses Table 1 to define this Expansion P-box. Since RI−1 is a 32-bit input and KI is a 48-bit key, we first need to expand RI−1 to 48 bits. C.
6) Perform XOR operation on the expanded right section (PTR) and the round key.
7) The S-boxes or Choice boxes perform the real mixing (or confusion) ensuring diffusion too.
8) DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. E. Straight P-box permutation (Simple transposition) to diffuse bits.
9) XOR output of P-box permutation obtained above with the PTR to produce new PT of right side (say PTR') and swap old PTR to become new PT of left side (say PTL'). Both PTL' and PTR' are of 32-bits.

IV. RESULTS

The results achieved by our methodology have been shown below. Table 1 show all the relevant details regarding the user data, password, status and comparison parameters value like time, space and attack status. Table 2 specifically shows the attack phenomena with the IP address and file name. As we are used the single system so the IP address is same. The encryption size and decoding size is same so there is no information misfortune in the event of literary information. This mechanism is shown in figure 2. The efficient virtualization mechanism is also shown in figure 3. In this we have adopted 500 KB + file size scheme for this mechanism. Means the space will automatically acquire the space 500 Kb + size of the files which is to be uploaded. Figure 4 shows the status of the attack to be done on the file before the data is received. It efficiently detect the time of attack also.

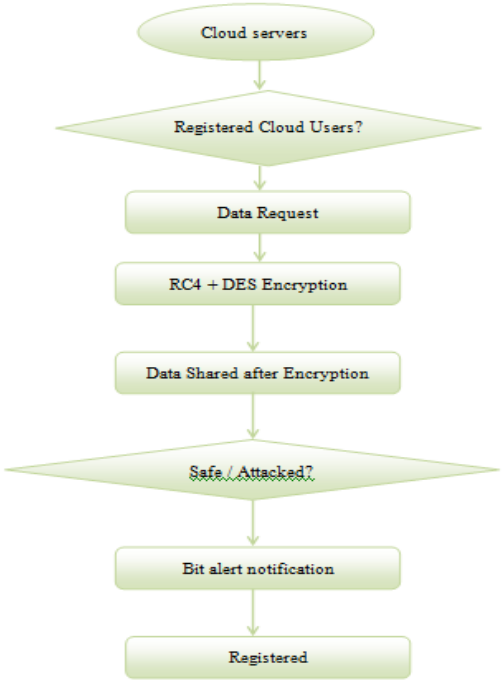

Figure 1: Working process

DOI 10.17148/IJARCCE.2015.4653

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Table 1: Log Table (a)

filename	username	server name	upload date	open	password	status
nt5.txt	abc12345	server4	Tue Jun 09 18:15:32 IST 2015	upload	kE9Hz4e8	safe
nt5.txt	abc1234	server4	Tue Jun 09 18:16:20 IST 2015	no	kE9Hz4e8	safe
dt1.txt	abc1234	server1	Tue Jun 09 17:45:36 IST 2015	upload	rT9Xh4f1	safe
dt1.txt	abc123456	server4	Tue Jun 09 17:54:04 IST 2015	yes	rT9Xh4f1	safe
ct1.txt	abc12345	server4	Tue Jun 09 17:49:03 IST 2015	upload	jF2Pg5b1	safe
ct1.txt	abc123456	server4	Tue Jun 09 17:55:13 IST 2015	yes	jF2Pg5b1	safe
ct1.txt	abc1234	server4	Tue Jun 09 17:55:21 IST 2015	no	jF2Pg5b1	attack
doc1.doc	abc12345	server4	Tue Jun 09 18:09:09 IST 2015	upload	qV5Od0z7	safe
nt2.txt	abc12345	server4	Tue Jun 09 17:50:22 IST 2015	upload	lJ2Nu8l9	safe
nt2.txt	abc123456	server4	Tue Jun 09 18:03:10 IST 2015	no	lJ2Nu8l9	safe
nt1.txt	abc1234	server4	Tue Jun 09 17:46:49 IST 2015	upload	eE2Ny3n1	safe
nt1.txt	abc123456	server4	Tue Jun 09 18:02:24 IST 2015	no	eE2Ny3n1	attack
nt3.txt	abc123456	server4	Tue Jun 09 18:01:38 IST 2015	upload	qJ6Pp1m8	safe
nt3.txt	abc12345	server4	Tue Jun 09 18:03:44 IST 2015	no	qJ6Pp1m8	attack

Table 1: Log Table (b)

encrys	decrys	encryt	decryt	encrysDES	decrysDES	encrytDES	decrytDES	keyDES
536	0	0	0	0	0	0	0	cE2Zp6w2
536	536	19	0	544	536	85	0	cE2Zp6w2
8927	0	0	0	0	0	0	0	cG0Ia3c7
8927	8927	72	2	8928	8927	2651	5	cG0Ia3c7
70476	0	0	0	0	0	0	0	eK1Ld9l5
70476	70476	26	46	70480	70476	43	70	eK1Ld9l5
70476	70476	35	0	70480	70476	45	0	eK1Ld9l5
23040	0	0	0	0	0	0	0	kT3Cw7b0
10457	0	0	0	0	0	0	0	lV5Iw6s8
10457	10457	60	0	10464	10457	69	0	lV5Iw6s8
16203	0	0	0	0	0	0	0	yF3Ig7v4
16203	16203	59	0	16208	16203	64	0	yF3Ig7v4
14263	0	0	0	0	0	0	0	zK4Gq1u7
14263	14263	55	0	14264	14263	58	0	zK4Gq1u7

Table 2: Attack Table

username	FILENAME	atttime	Alerttime	diff	ipaddress
abc1234	ct1.txt	Tue Jun 09 18:06:10 IST 2015	Tue Jun 09 18:06:10 IST 2015	62	192.168.1.101
abc12345	nt3.txt	Tue Jun 09 18:06:27 IST 2015	Tue Jun 09 18:06:27 IST 2015	49	192.168.1.101
abc123456	nt1.txt	Tue Jun 09 18:06:38 IST 2015	Tue Jun 09 18:06:38 IST 2015	71	192.168.1.101
abc1234	ct1.txt	Tue Jun 09 18:17:09 IST 2015	Tue Jun 09 18:17:09 IST 2015	88	192.168.1.101

DOI 10.17148/IJARCCE.2015.4653

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

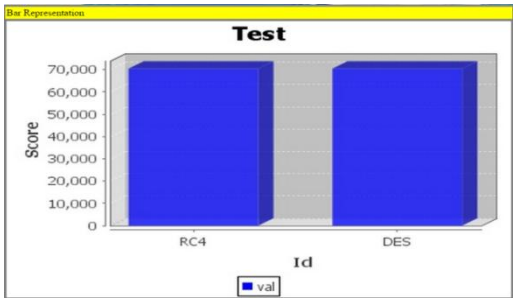

Figure 2: Encrypted File Size

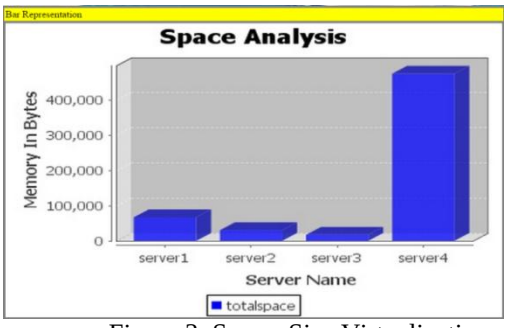

Figure 3: Server Size Virtualization

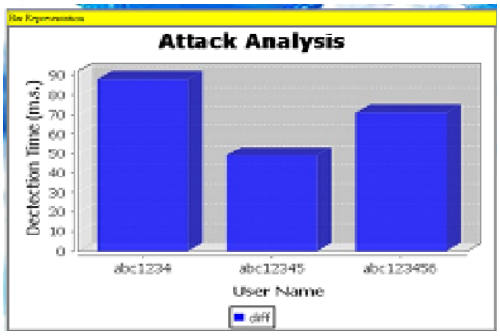

Figure 4: Attack Analysis

V. CONCLUSION

According to the study and investigation by the survey suggested in the manuscript is the securely data communication need in cloud environment. The more prominent request because of adaptability, interoperability, pay per utilization and virtualization and so forth. The security in distributed computing is the significant concern as the utilization of distributed computing is increments step by step. So according to our investigation a crossover structure is expected to secure the common information. In this regard we have developed a hybrid framework based on RC4 and DES mechanism to secure the data from unauthorized access in the cloud.

REFERENCES

[1] Tianfield, H., "Security issues in cloud computing," Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on , vol., no., pp.1082,1089, 14-17 Oct. 2012.

[2] Igor Ruiz-Agundez, Yoseba K. Penya and Pablo G. Bringas, "Cloud Computing Services Accounting", International Journal of Advanced Computer Research (IJACR) ,Volume 2, Number 2, June 2012.

[3] Ajey Singh, Maneesh Shrivastava, "Overview of Security issues in Cloud Computing", International Journal of Advanced Computer Research (IJACR) Volume 2,Number 1,March 2012.

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava," Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG-2012.

[5] A. Juels and B.S. Kaliski Jr., "Pors: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007.

[6] Sampada Kembhavi and Gajendra Singh, "Auto Upload and Chi-Square Test on Application Software as a Service for Cloud Computing Environment", International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014, pp.26-31.

[7] Kembhavi, Sampada, Ravindra Gupta, and Gajendra Singh. "An Efficient Algorithm for Auto Upload and Chi-Square Test on Application Software." nternational Journal of Advanced Computer Research (IJACR) volume 3, Issue 10 (2013).

[8] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya , "Service-Oriented Cloud Computing Architecture" , 2010 Seventh International Conference on Information Technology.

[9] G K Patra, Nilotpal Chakraborty," Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques", International Journal of Advanced Computer Research (IJACR) ,Volume-4 Number-1 Issue-14 March-2014.

[10] Nilesh Pachorkar, Rajesh Ingle," Multi-dimensional Affinity Aware VM Placement Algorithm in Cloud Computing", International Journal of Advanced Computer Research (IJACR) Volume-3 Number-4 Issue-13 December-2013.

[11] Adigun A. Adebisi, Adegun A. Adekanmi, Asani E. Oluwatobi, " A Study of Cloud Computing in the University Enterprise " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.450-458.

[12] Tschinkel, Brian. "Cloud Computing Security Understanding Risk Areas & Management Techniques." (2011).

[13] Abuhussein, A.; Bedi, H.; Shiva, S., "Evaluating security and privacy in cloud computing services: A Stakeholder's perspective," Internet Technology And Secured Transactions, 2012 International Conference for, vol., no., pp.388,395, 10-12 Dec. 2012.

[14] Wentao Liu, "Research on cloud computing security problem and strategy," Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on , vol., no., pp.1216,1219, 21-23 April 2012.

[15] Pant, N.; Parappa, S., "Seeding the cloud in a secured way: Cloud adoption and security compliance assessment methodologies," Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on, vol., no., pp.305, 308, 23-25 May 2013.

[16] Du meng," Data security in cloud computing", The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka.

[17] Fan Yang; Li Pan; Muzhou Xiong; Shanyu Tang, "Establishment of Security Levels in Trusted Cloud Computing Platforms," Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing , vol., no., pp.2119,2122, 20-23 Aug. 2013.

[18] Khalil, I.M.; Khreishah, A.; Bouktif, S.; Ahmad, A., "Security Concerns in Cloud Computing," Information Technology: New Generations (ITNG), 2013 Tenth International Conference on , vol., no., pp.411,416, 15-17 April 2013.

[19] Benameur, A.; Evans, N.S.; Elder, M.C., "Cloud resiliency and security via diversified replica execution and monitoring," Resilient Control Systems (ISRCS), 2013 6th International Symposium on, pp.150, 155, 13-15 Aug. 2013.

[20] Liu Xiao-hui; Song Xin-fang, "Analysis on cloud computing and its security," Computer Science & Education (ICCSE), 2013 8th International Conference on, vol., no., pp.839,842, 26-28 April 2013.

[21] Pareek, Astha, and Manish Gupta. "Review of data mining techniques in cloud computing database." International Journal of Advanced Computer Research (IJACR) Volume 2, Issue 4 (2012).

[22] Brahman, Sanjay Kumar, and Brijesh Patel. "Java Based Resource Sharing with Secure Transaction in User Cloud Environment." International Journal of Advanced Computer Research (IJACR), volume 2, Issue 5, 2012.

[23] Gupta, Saket. "Secure and Automated Communication in Client and Server Environment." International Journal of Advanced Computer Research (IJACR), volume 3, Issue 13(2013).