International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 – No. 8, November 2017 – www.ijais.org

Enhancing Security of Cloud Computing by using RC6 Encryption Algorithm

Salim Ali Abbas, PhD
Professor
Department of Computer Science
College of Education
Al-Mustansiryah University
Baghdad- Iraq

Malik Qasim Mohammed
Department of Computer Science
College Of Education
Al-Mustansiryah University
Baghdad- Iraq

ABSTRACT
Cloud computing give an impression of being an extremely well known and famous computing technology. Each person is utilizing cloud computing straightforwardly or indirectly such as email that usually utilized as an application of cloud computing. Everyone can get to the mail anyplace whenever. The email account is not obvious on personal PC but rather a person need to get to his account with the assistance of web. Like an email cloud computing give numerous different services, for example accessing to various applications, saving of any sort of information and so on. Clients can normally access and store information without fearing over how these services are given to client. Because of this adaptability everybody is exchanging information to the cloud, to store information on cloud client needs to send their information to the third party who will oversee and store information, so it is crucial for an organization to secure that information. Most difficult part is how to protect these data in light of the fact that these information can store anyplace in the cloud. This paper presents the proposed cryptographic algorithm used to address this issue.

General Terms
Cloud Computing, Security, Cryptography, Algorithms

Keywords
Cloud Computing, Encryption, Decryption, RC6 algorithm

1. INTRODUCTION
Cloud computing refers to sharing of assets instead of having local servers to deal with applications. It gives applications, storages over the web and services to servers. Environment of cloud computing is utilized by all little and big organization clients and there are many variables supporting cloud computing like virtualization, capacity, network and server. However, the real downside is security in giving information over the web. Every single cloud searcher is bringing up an issue to cloud supplier that whether it includes security approaches and methods before hosting their applications. Because of low security there exists poor API, information misfortune, hijacking and so on [1].

2. CLOUD COMPUTING MODELS
Cloud computing is an expression utilized to summery an assortment of computing ideas that includes massive associated PCs through communication network. Cloud computing has Enhanced calculation's effectiveness while lessening its cost for clients. Models of Cloud computing can arranged into 2 main categories as shown below [2], [3]:

2.1 Service Model
Providers of cloud computing found for providing services of cloud to all costumer through the web, these models can be arranged into SPI Model (software, Platform and Infrastructure).

A. Software as a Service (SaaS)

This model gives the user the ability to utilize the applications that running on a cloud environment easily. The applications are open and can be reached from different customer gadgets through a thin customer interface, for example, a Web browser. In this model the purchaser does not oversee or control the hidden cloud framework including system, servers, OSs, capacity, or private application abilities also in this model a total application is offered to the client, as services on request. On the client's side, there is no requirement for interesting in servers or programming licenses, while for the supplier, the expenses are brought down, since just an application should be hosted and kept up.

B. Platform as a Service (PaaS)

In this model a layer of programming, or advancement environment is covered or encapsulated and provided as a service, whereupon other larger amounts of services can be manufactured. The client has the freedom or ability to construct his own specific applications, which keep running on the supplier's framework. To meet reasonability and scalability prerequisites of the applications, PaaS suppliers offer a predefined mix of application servers and operating system For example, LAMP (Linux, Apache, MySql and PHP), Google's App Engine and Force.com are famous examples of this model.

C. Infrastructure as a Service (IaaS)

Here the purchaser enable to rent capacities , hardware processing , networks and other key computing assets where the customer can deploy and run self-programming which can incorporate applications and OSs .

2.2 Deployment Model
The cloud computing environment consists of multiple types of clouds based on their deployment and use, these models can be listed as below:

A. Public cloud
Public Cloud is model where the services are given to the clients over Internet based on demand and pay for per utilize. They are administrated by vendors over the web, and administrations are offered on pay-per-utilize premise. Its principle benefits are Provides very versatile and solid applications quickly and at more moderate expenses, Amazon AWS and Microsoft Azure are famous Providers of this type.

B. Private cloud
This environment lives within the limits of companies and it is utilized specially for the company's advantages. These are regularly worked by IT office within the companies and it requires an abnormal state of endeavors and skill to oversee clouds within the company. Its principle benefits are gives high security and better controls of services.

C. Hybrid cloud
It is a mixture of a public and private clouds, in this type services are normally gives as either companies having private cloud which makes a relationship with public cloud for broadened services. In short words this type makes benefits of low cost of public cloud and high security of private cloud.

D. Community cloud
This type of cloud permits sharing of foundation between organization of same group or community.

3. RELATED WORKS

Various analysts have talked about the security challenges that are occurred in cloud computing. Security problems has assumed the most vital part in upsetting the acceptance or approval of Cloud Computing. The concept of information encryption idea was bring back in 1972 by IBM. At that point, this idea had been embraced by the U.S state as a standard encryption, Sana Belguith et. al [4] proposed in their article a new hybrid encryption algorithm which consists of combining symmetric algorithm to encrypt data and asymmetric algorithm to distribute keys , the data is encrypted by a symmetric algorithm. Then, the symmetric key distribution between cloud provider and authorized users is performed using an asymmetric algorithm, this combination helps to brings benefit from the efficient security of asymmetric encryption and high performance of symmetric encryption. Their results prove that the processing time of their lightweight algorithm is faster than state of the art cryptographic algorithms.

A.Tripathi & P.Yadav [5] they used an elliptic curve cryptographic schemes and RSA for cloud based applications. They provide evidence and experimental results to proof that an elliptic curve based public key cryptography is far better than RSA based schemes. They used ECDSA algorithm and compared its performance with RSA algorithm, their results shows that ECDSA algorithm is better than RSA as far as performance.

Also S.S. Khan & R.R.Tuteja [6] their plan is to enhance the cloud security as per cloud customer's requirement and to eliminate the concerns related with data privacy. Their proposed system uses combination of two security algorithms such DES & RSA algorithm to generate encryption when user uploaded the text files in cloud storage and using the inverse DES & RSA algorithm when user download file from cloud storage to generate decryption.

Nazar K.Khorsheed et. al [7] In this paper, an encryption algorithms has been proposed to secure the data stored within the cloud , these algorithms have been applied are RC5 and AES encryption algorithms , This makes the level of security and performance more flexible and providing the privacy and integrity to the users' identities .

B.Thimma Reddy et. al [8] They proposed a framework for cloud computing depending on two algorithms, its main goal is to provide security in cloud and protecting the data transmitted through various trusted channels by using encryption, these algorithms used are (BFT) algorithm that provides safety over multi cloud model and Blowfish algorithm, Encryption and decryption with Blowfish uses an ample amount of sub keys, their approach provides a better increasing in decreasing the threats on cloud computing.

Maha Tebaa & Said El Hajii [9] they propose a method to execute operations on encrypted data without decrypting them. They use a standard encryption methods to secure the operations and the storage of the data. They utilized Homomorphic encryption to applied operations on encoded information without knowing the secret key of the customer, the consequence of any operation, it is the same as though if completed the figuring on the crude information in decoding process .also this paper analyzes the application of different Homomorphic encryption cryptosystems (RSA, Paillier, El Gamal) on a cloud computing platform.

4. PROPOSED WORK

4.1 General Description of Proposed System

firstly the proposed system is build and developed to achieve and gains the properties of a secure and trusted environment, the idea of the proposed system is that we built an online application that supports the text only its main goal is to enabling the users to makes books, articles and papers online without needing to worry about the information status because the proposed system able to keep the user's information safe. The proposed system gives a unique ID and Password to each user , users of the proposed system can login to the system by their individual and private IDs and able to do a lot of things such are all what is concerns with articles, books and papers editing, from changing the contents and titles to the writing and printing options available by the system , when a user leaves for a reason , the information (text) never be lost and users can still continue what they has done previously when they are logging in the system once again , because the proposed system enabling its users to keep their information safe and secure and accessing to their information from anywhere, any time and from any device .Figure (1) illustrated the mechanism used by the proposed system to deal with user's data.

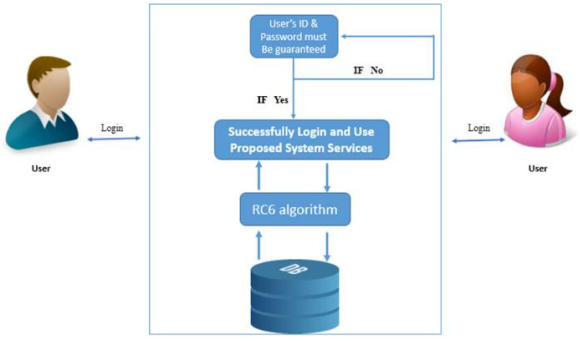

Fig 1: Proposed System mechanism to deal with data of users

After data is created by users of the proposed system, these data handled and treated with RC6 algorithm, then encrypted and stored in database through encryption process, as it shown in Figure (2).

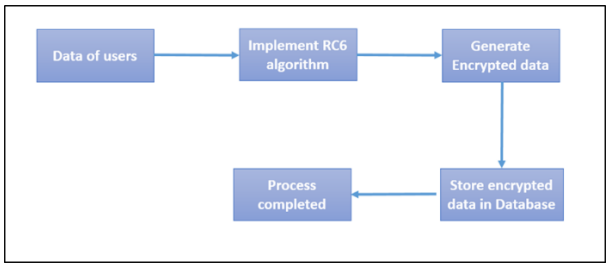

Fig 2: Proposed system mechanism to encrypt user's data

For the decryption process the user's encrypted data that stored in database are decrypted, the decrypted (original) data is retrieved and the decryption process is completed as shown in Figure (3). The data are still protected and secure while it is in database and no one have the right to reaches them except the authorized user that is previously proven his Identity.

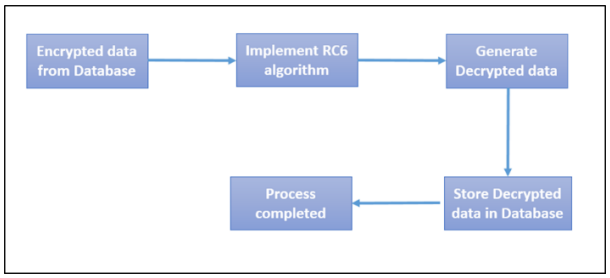

Fig 3: Proposed system mechanism to decrypt user's data

4.2 RC6 Encryption Algorithm

RC6 is a symmetric key algorithm in which encryption and decryption are performed utilizing a similar key, RC6 algorithm is a block cipher derived from RC5, It was outlined by Ron Rivest ,Matt Robshaw ,Ray Sidney and Yiqun Lisa Yin to meet the prerequisites of the (AES) algorithm [10], figure (4) shows a general diagram of RC6 algorithm .

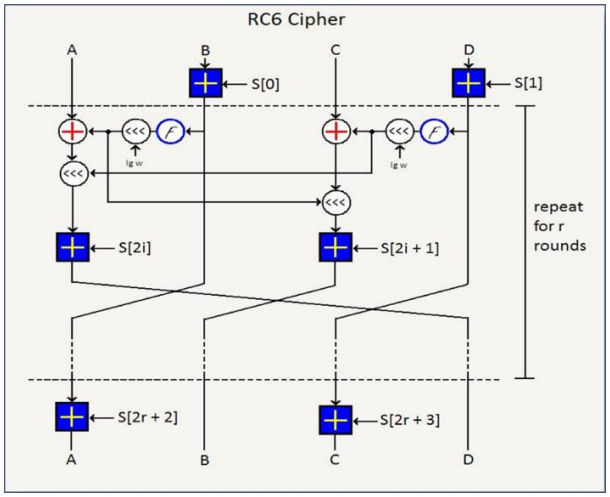

Fig 4: General Diagram of RC6 Algorithm

This algorithm is consist of three stages, which are:

A. The key expansion algorithm

The key expansion algorithm is utilized to grow the client provided key to fill an extended array S, so S looks like a variety of t random binary words, The client must supply a key of b bytes, where $0 \leq b \leq 255$, and from which (2r+4) words are inferred and put in a round key array S , Zero bytes are affixed to give the key length equivalent to a "non-zero integral number" .

The key bytes are then stacked in little endian arrange into a cluster L of size c : when b = 0, c = 1 and L[0] = 0 , e ="2.718281828459" and ø = "1.618033988749", Pw and Qw are "magic constants" and Odd(x) is the least odd integer greater than or equal to x , The (2r+4) determined words are put in array S for later encryption and decryption , Figure (5) illustrates the algorithm of the key expansion utilized in RC6 .

RC6 key expansion algorithm

INPUT:

User-supplied b byte key preloaded into the c-word array L[0,…, c - 1]
Number r of rounds
Pw = Odd((e – 2)2w)
Qw = Odd((ø – 1)2w)

OUTPUT:

w-bit round keys S[0,…, 2r + 3]

Procedure:

```
S[0] = Pw
for i = 1 to (2r + 3) do
S[i] = S[i _ 1] + Qw
A = B = i = j = 0
v = 3 x max{c, 2r + 4}
for s = 1 to v do
{
A = S[i] = (S[i] + A + B) <<< 3
B = L[j] = (L[j] + A + B) <<< (A + B)
i = (i + 1) mod (2r + 4)
j = (j + 1) mod c
}
```

Fig 5: Key Expansion Algorithm of RC6

B. Encryption process & Decryption process

After key expansion process is completed the next process is encryption stage, when the users wish to encrypt their information the proposed system will applied encryption algorithm and stores the encrypted information of the users in database, also the proposed system will apply decryption algorithm when user wish to decrypt these information to retrieve the plain text (Information) from the encrypted data that stored in database. The algorithms of this stage are illustrated in more details below in the Figure (6), (7).

RC6 Encryption algorithm

INPUT:

Plaintext stored in four w-bit input registers A,B,C,D

Number r of rounds

w-bit round keys S[0,…,2r + 3]

OUTPUT:

Cipher text stored in A,B,C,D

Procedure:

B = B + S[0]

D = D + S[1]

for i = 1 to r do

{

t = (B x (2B + 1)) <<< log2 w

u = (D x (2D + 1)) <<< log2 w

A = ((A ⊕ t) <<< u) + S[2i]

C = ((C ⊕ u) <<< t) + S[2i+ 1]

(A,B,C,D) = (B,C,D,A)

}

A = A + S[2r + 2]

C = C + S[2r + 3]

Fig 6: Encryption algorithm of RC6

RC6 Decryption algorithm

INPUT:

Cipher text stored in four w-bit input registers A,B,C,D

Number r of rounds

w-bit round keys S[0,…,2r + 3]

OUTPUT:

Plaintext stored in A,B,C,D

Procedure:

C = C - S[2r + 3]

A = A - S[2r + 2]

for i = r down to 1 do

{

(A,B,C,D) = (D,A,B,C)

u = (D x (2D + 1)) <<< log2 w

t = (B x (2B + 1)) <<< log2 w

C = ((C - S[2i + 1]) >>> t) ⊕ u

A = ((A - S[2i]) >>> u) ⊕ t

}

D = D - S[1]

B = B - S[0]

Fig 7: Decryption algorithm of RC6

5. RESULTS

There are number of threats and attacking programs [11],[12],[13] applied to the proposed system to check the system trustiness and to be quite sure of information security status, the results shows that the proposed system has a high resistance against these dangers and able to keep user's information safe , the overall results of threats and attacks that has been applied have no effect against user's private information, each one of these tests are includes number of threats or attacks and applied individually without effecting other tests . The security tests applied shows that the proposed system is protected against threats and vulnerabilities and there are no worry about user's information. Some of these security tests such are:

1. Web Inspector Test

Web Inspector is free website scanner that can detect security threats, attacks and gives an immediately report that includes information about Worms , Trojans, Malware, Suspicious associations and frames , Phishing , Backdoors and also Blacklist checking .Web Inspector checks the site for conceivable infection and malware contamination , recognizes the security vulnerabilities and gaps and protects the site against security dangers , additionally it screens for site blacklisting and instantly cautions the site proprietor before the site gets blacklisting .

Test result

The test is highlights number of threats and attacking Security loopholes to the proposed system, the result shows that the proposed system is protected against these threats and have no malicious activity or malware detected as shown in figure (8).

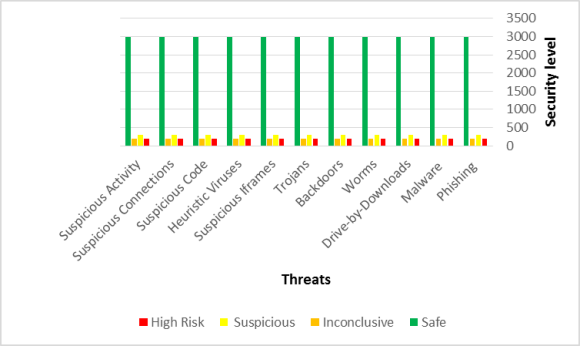

Fig 8: Web Inspector test result

2. Acunetix Test

Acunetix is free website scanner that tests a web applications and websites for: XSS, XXE, SSRF, Host header attacks and SQL Injection besides many others, beside that acunetix gives an impressive management tools for ensuring vulnerabilities not only founded but dealing with these vulnerabilities in reliable manner and fix them and provide a reports of a required steps to make the strategic decisions. The acunetix tests can be classified as three types of tests which are:

A. Crawl Only Test

Sometimes web crawler known as a spider, which is a technique that commonly browses the WWW for the purpose of Web indexing (spidering). some websites and different search engines utilizes Web spidering programs to refresh their web substance or lists of others destinations' web content , Web crawlers can duplicate every one of the pages they visit it for later preparing by search engine which lists the

downloaded pages so the clients can explore more productively .

Test result

The result shows that the proposed system is passed this test successfully and protected against these threats and have no malicious activity or malware detected as shown in figure (9).

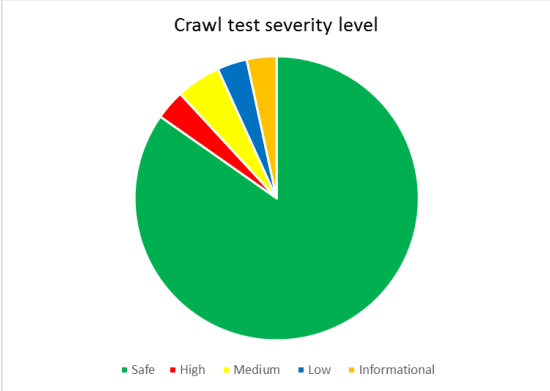

Fig 9: Crawl only Test Result

B. Cross-Site Scripting Vulnerabilities XSS Test

Cross site scripting (XSS) is a sort of PC security weakness ordinarily founds in a web applications, its purpose is to empower attackers to infuse customer side contents into site pages saw by different clients .XSS weakness might be utilized by attackers to sidestep get to controls, look like the same-root strategy. XSS impacts fluctuate in go from trivial aggravation to critical security hazard, depending upon the affectability of the information dealt with by the powerless site and the idea of any security moderation executed by the site's proprietor.

Test result

The result shows that the proposed system is protected against this threat and have powerful resistance against the XSS vulnerability as shown in figure (10).

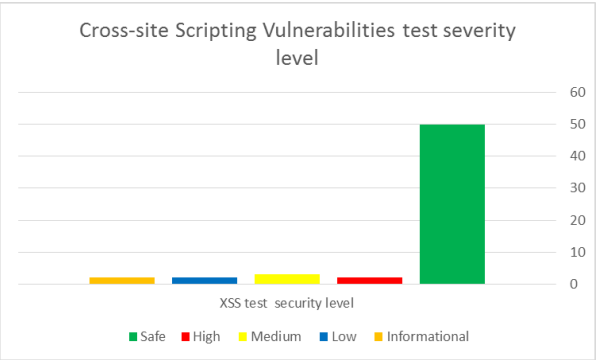

Fig 10: Cross-site Scripting Vulnerabilities Test Result

C. Weak Passwords Guessing Attack Test

Password quality is a measure of the viability of a Password against brute force or guessing attacks, in its typical frame it gauges what number of trials an assailant who does not have access to the password generally would require or needs to get it effectively, by other mean the quality of a password can be summarized by it is an element length, multifaceted nature and unconventionality. Utilizing solid passwords brings down general danger of a security break, however solid passwords doesn't cancel the needing requirement for other successful security controls, The adequacy of a secret word of a given quality is firmly controlled by the plan and execution of the elements (information, possession, inherence). Key factor to deciding the security of the system is the rate at which an assailant can perform the guessed passwords attack to the framework.

Test result

The result shows that the proposed system is detected one low-severity type (low risk) have been discovered by the scanner when applied this attack to the system as shown in figure (11).

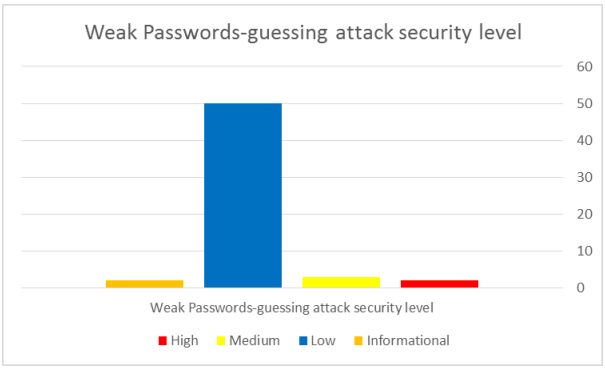

Fig 11: Weak Passwords guessing attack /security level

3. Quttera Test

Quttera is a free site scanner that can get malware discovery, webpage tidy up administrations, blacklisting checking and other fundamental instruments for the protected and trusted site, it is also offers SaaS based malware discovery solution for recognize obscure and ”zero day” dangers on sites and to give a constant cautioning to organizations and associations. Quttera can checks any site/area for web malware and web dangers, also provide a report with web dangers, malicious and hidden redirects, iframes, and distinguishes binary shell codes, JavaScript programming weakness uses, drive by download assaults, malware in media records, misuses in digital archives and different threats of malicious files and content planted in the normal documents.

Test result

The result shows that Quttera scan testing of the proposed system have no malicious and suspicious activity are detect, the test also detected one external link that bring back to URL of the proposed system, besides the test are scores a high rate of clean files as shown in figure (12) .

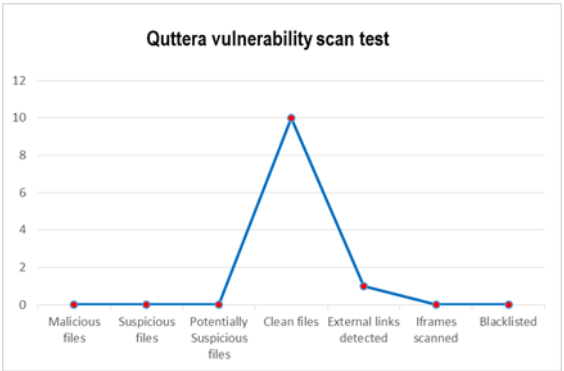

Fig 12: Quttera Vulnerability Testing Result

4. Gravity Scanner Test

Gravity is a free site scanner that can identifies malware and vulnerability to see whether a site has been hacked or has any security issues needs to be fixed, this test checks for any malware or vulnerability can be found.

Test result

The result shows that the proposed system have passed the three tests (malware , vulnerability and content) successfully and nothing are detected, the results also shows that the test discover one low severity level concerns with the URL of the proposed system as shown in figure (13) .

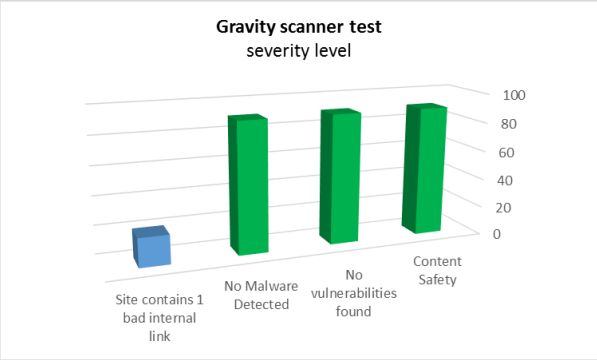

Fig 13: Gravity Scan testing result

6. CONCLUSION

RC6 algorithm has been proposed to enhance the level of security for the data stored by user within the cloud. This algorithm has been applied on the proposed system to gains the properties of trusted environment. The suggested algorithm and the proposed system shows the resistance against the known attacks that have been used to measure the performance of this algorithm. The results indicated that the performance of the proposed algorithm views the ability to protect user's data against threats and attacks. Furthermore, this algorithm can be enhanced by adding another encryption technique such are RC7 to increase the security level and to prevent the hacker's activities. Also, other features can be added to the proposed algorithm such are using the artificial intelligence with the proposed system.

7. ACKNOWLEDGMENTS

I highly appreciate the efforts expended by my supervisor Prof Dr. Salim Ali Abbas for his encouragement, and I am so grateful for his support and advise.

8. REFRENCES

[1] V.Masthanamma, G.Lakshmi Preya,"An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm" , International Journal of Innovative Research in Science Engineering and Technology , Vol. 4, Issue 3, March 2015 .

[2] Poonam Rani, Kavita Taneja, "Service and Deployment Models for Cloud Computing Environment", International Journal of Enhanced Research in Science Technology & Engineering, Vol. 3 Issue 1, January-2014, Available online at: www.erpublications.com.

[3] Kanika Gulati, Kamal Kumar, Sharad Chouhan, "Cloud Computing & Its Deployment Models" , International Journal of Recent Research Aspects Feb 2015.

[4] Sana Belguith ,Abderrazak Jemai , Rabah Attia," Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm" , The Eleventh International Conference on Autonomic and Autonomous Systems, 2015 .

[5] Abhuday Tripathi , Parul Yadav, " Enhancing Security of Cloud Computing using Elliptic Curve Cryptography", International Journal of Computer Applications ,Volume 57– No.1, November 2012 .

[6] Shakeeba S. Khan, R.R. Tuteja, " Security in Cloud Computing using Cryptographic Algorithms" , International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2015 .

[7] Nazar K. Khorsheed, Omeed K.Khorsheed, Majdi Z. Rashad,Taher T. Hamza, " Proposed Encryption Technique for Cloud Applications" , International Journal of Scientific & Engineering Research, Volume 6, Issue 9, September 2015 .

[8] B.Thimma Reddy, K.Bala Chowdappa, S.Raghunath Reddy, " Cloud Security using Blowfish and Key Management Encryption Algorithm" , International Journal of Engineering and Applied Sciences (IJEAS), Volume-2, Issue-6, June 2015 .

[9] Maha TEBAA, Said EL HAJII, " Secure Cloud Computing through Homomorphic Encryption" , International Journal of Advancements in Computing Technology(IJACT) Volume5, Number16, December 2013 .

[10] Vikas Tyagi , Shrinivas Singh , " Enhancement Of RC6 (Rc6_En) Block Cipher Algorithm And Comparison With RC5 & RC6 " , Journal of Global Research in Computer Science , Volume 3, No. 4, April 2012 .

[11] Comodo Web Inspector , Administrator Guide Version 1.0, also it available on https://help.comodo.com/uploads/helpers/Comodo_Web_Inspector_Admin_Guide.pdf.

[12] Acunetix Web Vulnerability Scanner User Manual V7, March 2011, also it available on https://www.acunetix.com/resources/wvs7manual.pdf.

[13] Russ McRee , OWASP ZAP – Zed Attack Proxy , Information Systems Security Association (ISSA) 2011 , also it available on https://holisticinfosec.org/toolsmith/pdf/november2011.pdf.