IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. V (Sep.- Oct. 2017), PP 51-56
www.iosrjournals.org

Improving Data Storage Security in Cloud Computing Using RC6 Algorithm

Prof. Dr. Salim Ali Abbas*Malik Qasim Mohammed*
**Department Of Computer Science, College Of Education, Al-Mustansiryah University*

Abstract: *In spite of the huge advantages got from the selection of cloud computing idea, its famous adoption has been determined usually by security concerns. The broadened assault surface in a cloud environment makes it more defenseless against existing and developing security dangers. Customary information security approaches have been discovered inadequate in abridging these dangers and this obnoxious pattern has required the requirement for an advanced methodsto deal with datasecrecy. This paper proposes an improved component to guaranteeing information security by utilizing RC6algorithm. we went for utilizing the quality of these techniques to gains a powerful instrument for guaranteeing secrecy and integrity of information in the cloud .The results obtained from proposed system shows that ability to resistance the threats and attacks and able to keep user's data secure and trusted .*

***Key words**: Cloud Computing , Encryption , Cryptography , RC6 algorithm*

Date of Submission: 25-09-2017 Date of acceptance: 04-11-2017

I. Introduction

Cloud computing is another PC demonstrate that permits utilizing remote services through a system utilizing different assets. It is fundamentally intended to give the most extreme limit with the minimal resources. The end client has the limithardware necessity, however he utilizes the most extreme capacity of computing. This is conceivable just through this concept which requires and uses its resources in the most ideal way. Cloud computing gives IT benefits as on request and ability to reaches them from anyplace, anytime and by approved client [1] .

A. Definitions

Cloud Computing is an internet based computing where virtual shared servers give programs , framework , platform , gadgets and different resources and hosting to clients depending on what things has been used . the data in the Cloud Computingmodel is provided as a services, Clients can get to these services accessibleon the " Internet cloud " without having any past know how on dealing with the resources included [2] . There are a huge definitions of Cloud Computing , such as David W. Cearley defines Cloud Computing as " Cloud is a style of computing where scalable and elastic IT-related capabilities are provided as a service to external customers using Internet technologies " [3] .

The famous definition that has known over world wide is the NIST definition which is : "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or Service Provider (SP) interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models " [4] .

B. Essential Characteristics of Cloud Computing

Essential characteristics of Cloud Computingcan be arranged as [5]:

- On-Demand Self-Service: On-demand self service allows clients to utilize Cloud Computing resources as required without the interaction between the CSP and client by human . With On-demand self-service , ashopper can plan the utilization of cloud services , for example, computation and capacity as required, inexpansion to overseeing and deploying these services. Keeping in mind the end goal to be viable and satisfactory to thepurchaser, the self-service interface must be easy to understand and give viable intends to deal with the service offerings , this gives efficiencies and reduces cost funds to both the client .
- Broad Network Access : For Cloud Computing to be a compelling contrasting option to in-house data centers , high-transmission capacity communication joins must be accessible to associate with the cloud services . the biggest economic advantages of Cloud Computing is that the brought down cost of high data

transmission network communication to the CP access to a bigger pool of IT resources that manage a bigger level of use .

- Location Independent Resource Pooling : The cloud must have an expansive and adaptable resource pool to meet the buyer's needs, give economies of scale, and meet service level prerequisites. Applications desires resources for their implementing , and these resources must be apportioned effectively for ideal execution , The resources can be physically situated at numerous geographic areas and alloted as virtual parts of the computation as required .
- Rapid Elasticity : Rapid elasticity alludes to the cloud ability to extend or diminish allocated resources by fast way and productively to meet the necessities of the self service characteristic for Cloud Computing .
- Measured Service : by using service-oriented characteristics of Cloud Computing , cloud resources utilized by a purchaser can be automatically and dynamically allotted and monitored . The client can then be charged in view of the deliberate use of only the cloud resources that were allotted for the specific session .

II. Related Works

This section emphasize recent researches in cloud data storage,**Dr. Salim Ali**&**Amal AbdulBaqi**[6] in their paper aims to provide a secure, effective and flexible method to improve data storage security in cloud computingBy using IBC to decrease the complexity of key management, also they use ofElliptic curve cryptography(ECC)algorithm to provides data secrecy and use Elliptic curve digital signature (ECDS)algorithm to provides data integrity.

Balkees Mohamed et. al [7] they focused in their paper to provide a new method for Cloud Computing Security by applying RSA algorithm and Fermat’s theorem together to keep user’s data highly secured against unauthorized servers and from malicious dangers. Their purposed workusing Fermat’s theorem to speed up the RSA Encryption and helping to build a new trustedenvironmentof cloud computing.

Punam V.Maitri & Aruna Verma[8]they discuss in their paper a problem statement When storing the data on cloud there are number of issues. The mainissues of cloud computing are data security, integrity, authentication and confidentiality,they makes the survey of different symmetric and asymmetric algorithms to provide the solution for these security issues.

Vibhey Bhangotra & Amit Puri[9] in their paper trying to solve cloud computing challenges such data safeness and access control when customers outsource delicate data for sharing on cloud servers , they used combination of symmetric techniques like message Digest encryption (MD5), AES encryption andRC5 algorithm . Theirproposed scheme analysis shows that proposed scheme is efficient and secures security models.

Sonia Arora&Pawan Luthra[10] they proposed a security model for data storage to eliminate Security and trust problems in cloud. theirproposedsystem provides security for data by using encryptionalgorithms,one algorithm will be chosen from eight algorithms such are RC6, RC4, Blowfish, AES and others to encrypt the file then transfer it to cloudand using hashing algorithms to checks integrity.

A.R.Zadeet. al [11] proposed a System modelof Cloud storage by using Partitioning function that plays amajor role in this workbecause it breaks larger files into smaller parts to store the data efficiently and enhancing the access to data storage. Then partitioned files are encrypted using RC6 Algorithm and SPEKE algorithm for key exchange and storedin cloud.

A suggested method to build a trusted computing environment for Cloud Computing storage by **Mehak & Gagandeep**[12] providing secure cross platform into cloud computing using Hadoop and AES encryption algorithm , Hadoop method which is a popular approach to together many low end machines together as a single functional distributes system ,The experimental results shows the effectiveness of this methodology to improve the security of data in cloud environment.

III. Proposed Work

1. General Description Of Proposed System

At first we must mention that the proposed system build and developed to achieve and gains the properties of a secure and trusted environment, the idea 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.

When the information is created by users of the proposed system , proposed system deals with these information very carefully and encapsulated them for later encryption and decryption processes .Figure(1) shows a general diagram of the proposed system

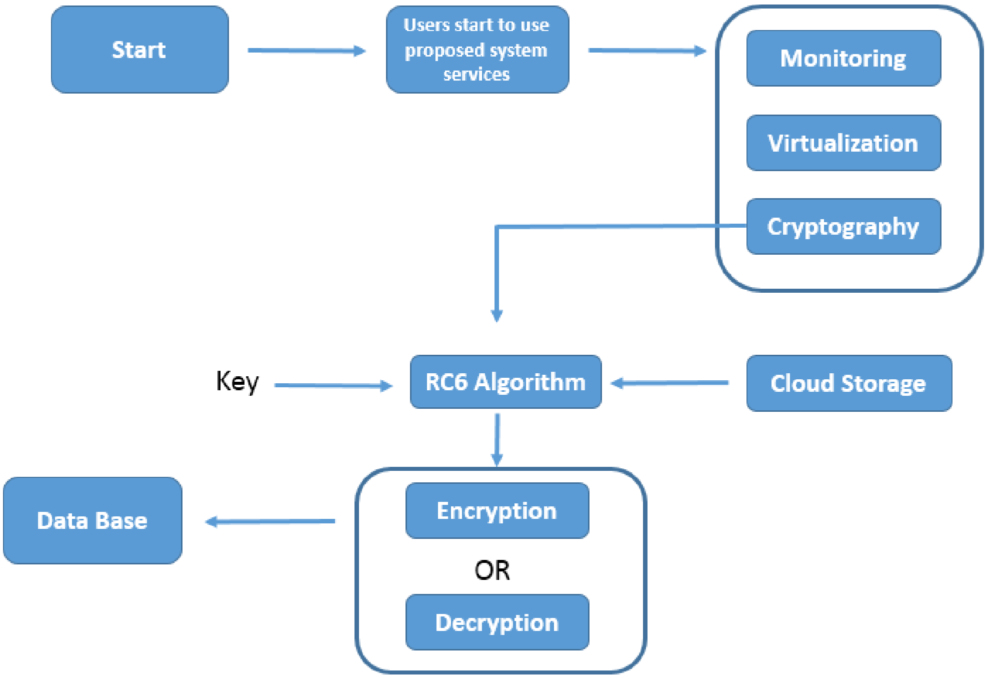


Figure 1: *General Proposed System Diagram*

The proposed system provide many services to its users but in this research we focused on security side , the user's information are encrypted with RC6 algorithm and stored in database through encryption stage, and these encrypted information are decrypted after it back from database to retrieve the original information through decryption stage as it shown in figure (2) .

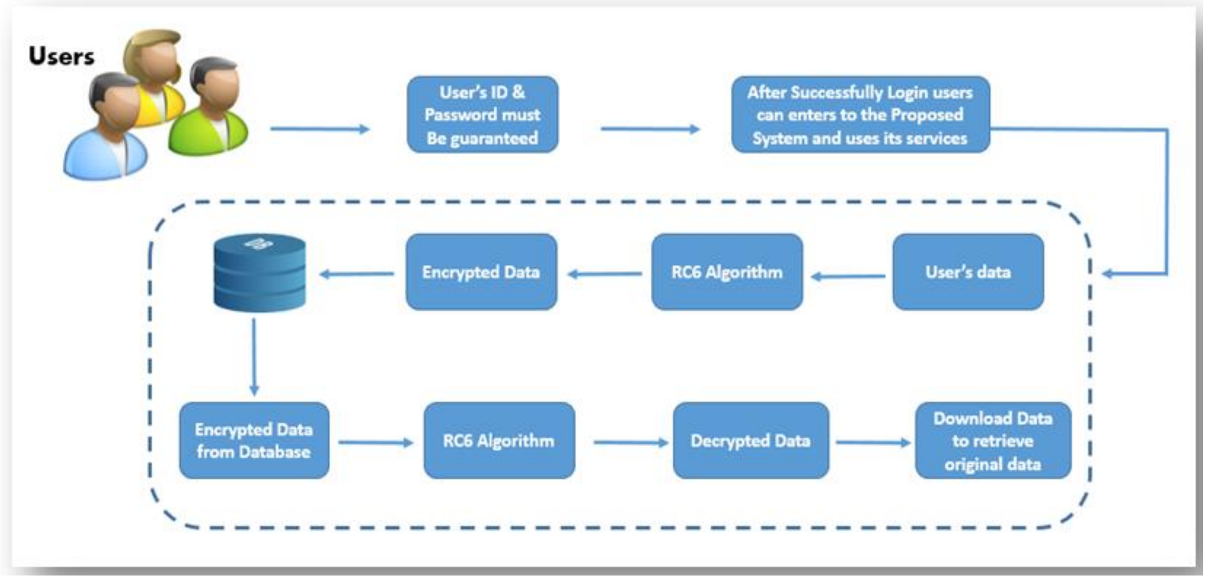

Users
User's ID & Password must Be guaranteed
After Successfully Login users can enters to the Proposed System and uses its services
Encrypted Data
RC6 Algorithm
User's data
Encrypted Data from Database
RC6 Algorithm
Decrypted Data
Download Data to retrieve original data

Figure 2: *Details Proposed System Diagram*

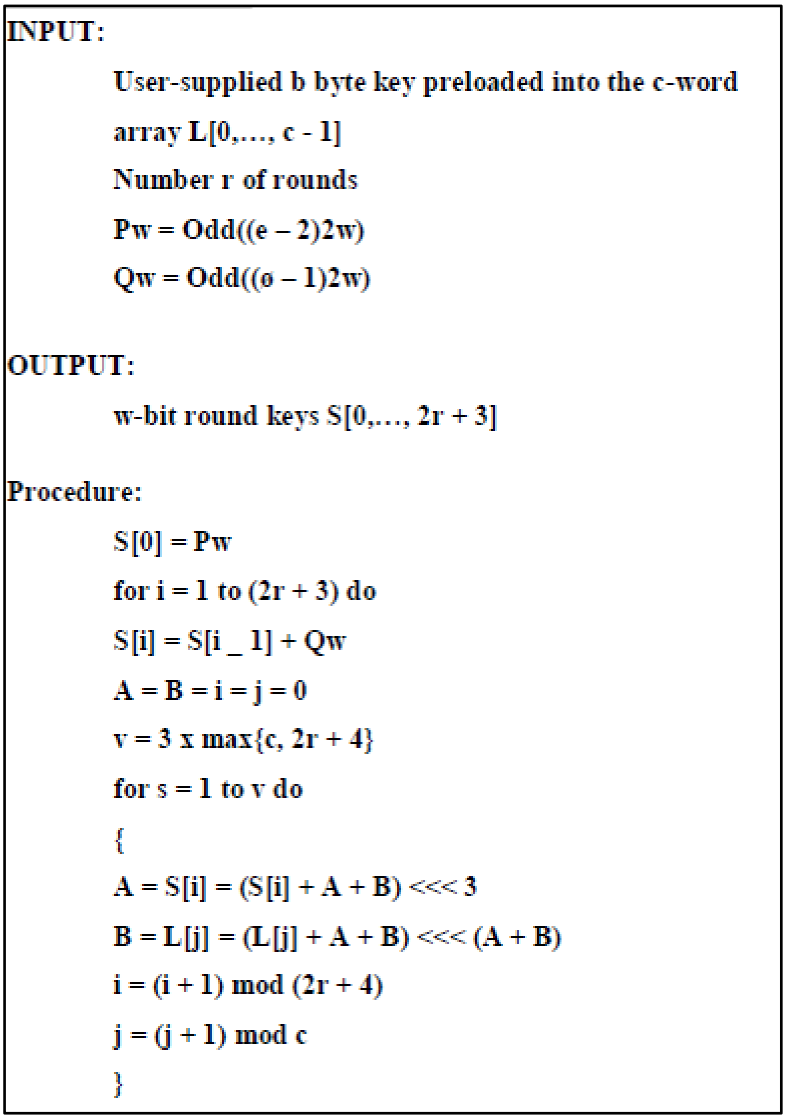
2. RC6 Encryption Algorithm

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]. 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 ≤ b ≤ 255, and from which (2r+4) words are inferred and put away in a round key array S , Zero bytes are affixed to give the key length equivalent to a "non-zero integral number" .

The (2r+4) determined words are put in array S for later encryption and decryption , Figure (3) illustrates the algorithm of the key expansion utilized in RC6 .

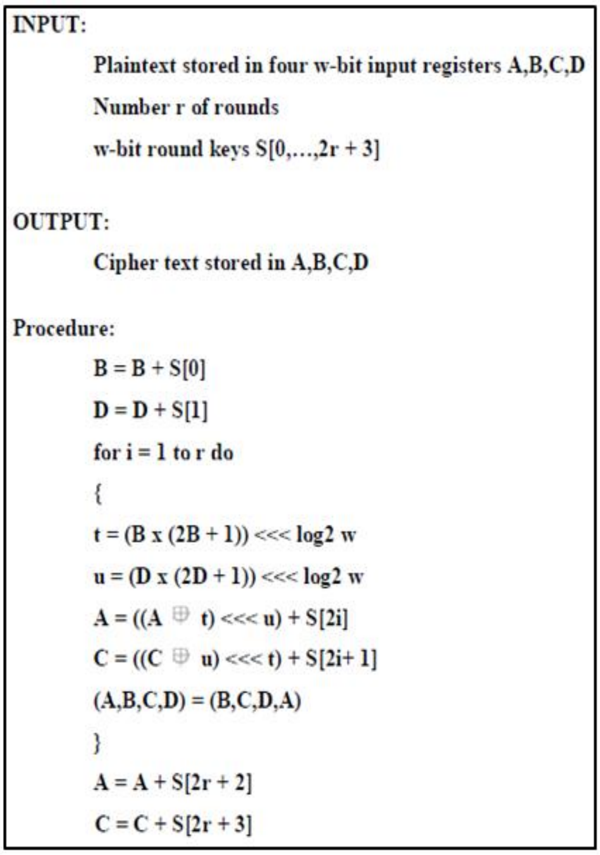


```
INPUT:
        User-supplied b byte key preloaded into the c-word
        array L[0,…, c - 1]
        Number r of rounds
        Pw = Odd((e – 2)2w)
        Qw = Odd((ø – 1)2w)

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
        }
```

Figure3: *key expansion algorithm of RC6 which is used in the proposed system*

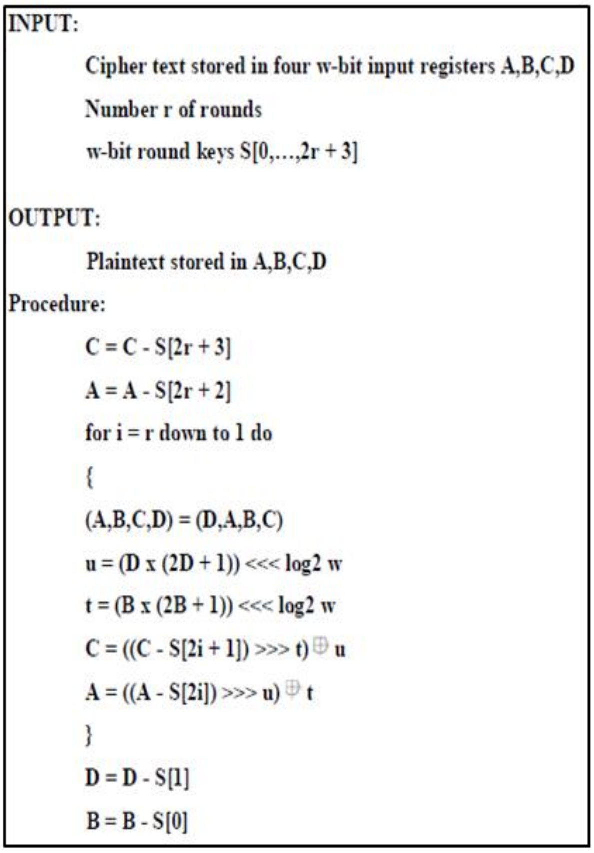
B. Encryption process & Decryption process

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 this algorithm and stores the encrypted information of the users in database, also the proposed system will apply decryption algorithmwhen user wish to decrypt these information to retrieve the plain text (Information) from the encrypted data that stored in database . these algorithms of this stage are illustrated in more details below in the Figure (4),(5).



```
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]
```

Figure4: Encryption algorithm of RC6



```
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]
```

Figure5: Decryption algorithm of RC6

IV. Conclusion And Future Work

Symmetric algorithms are gives better performance in terms of speed as compare to asymmetric algorithm while Asymmetric algorithms provide better security as compare symmetric algorithm.RC6 algorithm gives better performance in terms of speed as compare to AES algorithm but AES algorithm require minimum amount of time for encryption and decryption as compare to RSA .In future we will introduce new cryptography algorithm to avoid the security risk in cloud computing and improve the quality of service such using BlowFish algorithm .

References

[1] Zaid Kartit, Mohamed El Marraki , "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage",(Advance online publication: 17 November 2015) .

[2] Luit Infotech, "What Is Cloud Computing? " also it available on online Website: http:// www.luitinfotech.com .

[3] Gartner, Cloud Computing : Key Initiative Overview , 2010 .

[4] Peter Mell , Timothy Grance " The NIST Definition of Cloud Computing" September , 2011 .

[5] Ronald L. Krutz, Russell Dean Vines , " Cloud Security : A Comprehensive Guide to Secure Cloud Computing" , 2010 .

[6] Prof. Dr. Salim Ali Abbas, AmalAbdulBaqi ,"Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography" ,Journal of Computer Engineering (IOSR-JCE)Volume 17, Issue 4, Ver. I (July – Aug. 2015 .

[7] Balkees M. Shereek, ZaitonMuda, SharifahYasin , "Improve Cloud Computing Security Using RSA Encryption WithFermat's Little Theorem" , IOSR Journal of Engineering (IOSRJEN) ,Vol. 04, Issue 02 (February. 2014).

[8] Punam V.Maitri , Aruna Verma , "Enhancing File Security using CryptographyAlgorithms in Cloud Computing: A Survey" , International Journal of Innovative Research in Computerand Communication EngineeringVol. 3, Issue 10, October 2015.

[9] Vibhey Bhangotra, Amit Puri, "Enhancing Cloud Security By Using Hybrid Encryption Scheme" , International Journal of Advanced Engineering Technology ,(IntJAdvEnggTech)Vol. VI/Issue IV/2015.

[10] Sonia Arora, Pawan Luthra, "Security Storage Model Of Data In Cloud" , International Journal Of Current Engineering And Scientific Research (IJCESR) VOLUME-2, ISSUE-6, 2015 .

[11] A.R.Zade, Shaikh Umar, Potghan Rahul, Rale Sagar , Borade Sagar ,"Improving Cloud Data Storage Using Data Partition and Recovery",International Journal Of Engineering And Computer Science Volume 4 Issue 1 January 2015.

[12] Mehak, Gagandeep ,"Improving Data Storage Security in Cloud using Hadoop" ,Journal of Engineering Research and Applications, Vol. 4, Issue 9, September 2014.

Prof. Dr. Salim Ali Abbas Improving Data Storage Security in Cloud Computing Using RC6 Algorithm." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017, pp. 51-56.