ISSN No. 0976-5697

Volume 6, No. 6, June - July 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# A Research on Cloud Computing Security with RC5 Algorithm

Harmanjeet Kaur
M. Tech Computer Science
Punjab Technical University, India

Ms. Neha Bhardwaj
AP, M.Tech Computer Science,
Department of CSE

***Abstract:***Cloud computing has different meaning to different people, the privacy and security issues also differ between a consumer using a public cloud application, a medium-sized Company using a customized Design of business on a cloud platform, and Some Companies are using Platform on Public level which are Public to Public Network The security requirements in cloud computing environment is to find the Security threats in the Structure of clouds To find the security solutions, and finding Reason so that Pre Security Step Should be taken in concerned with security proposed model. In this paper we proposed the algorithmfor data encryption technique

***Keywords:*** cloud computing,data breaches,Api Attack Deniel Attack,Account high Jacking,Deniel of Services

## I. INTRODUCTION

Cloud computing concept is most important in today's world .It is important for both user and developers because of many important services it provided [1].It is found that cloud computing will be very important concept in future because it act as an infrastructure to all the services [6].Cloud Computing is used in almost every field which relates to computer such as it is used in Medical,In case of engineering etc . [2].The cloud computing provides many features to computer and information applications .The term cloud has been found from complicated infrastructure [3].Cloud Computing is the newest technology in field of Information technlogy .Because of its new technology It is difficult for both the Producer and consumer to use it. Therefore in recent days cloud computing has become a major challenging issue [1]. The most challenging issue is the use of cloud computing[7]. Cloud computing provide the facility to access shared resources and also provides the facility to share resources whenever required by the user. [1].

In the area of Cloud Computing different Security models and algorithms are available. These security models are not fully applicable to Solve all the threats and it can be use in field of online business . The Security provided in cloud is very cost effective process but cloud have full ability to shared resources on the network so that the users use these resources whenever required [1]The encryption technique is very important technique while providing security to data sharing so that the threats can't be occurred and data integrity is maintained so we have to improve the level of encryption. [5].

We use various security algorithm to provide message security using session key . These algorithms first encrypt the message to be transmitted [1]The steps which are used to inform encryption and decryption are same but the order in which these two functions are performed is different. Secondly the message digest hash function is available with cryptographic hash function approach with 128 bit fixed length..for eg if at one time the network digest 89 bits message then we must send 89 bit message in order to send it properly. Append Padding Bits

a. Append Length
b. Initialize MD buffer
c. Process message in 16-word blocks
d. Output

The main work of message digest so for this reason if the hacker can have full acess on network but he cant able to retrieve the password. [1].

### *A. Related Concepts about Cloud:*

#### *a. Deployment Cloud Models:*

***a) Public cloud:*** This is a cloud infrastructure which is available to public as well as large industries through internet connection [1].

***b) Private cloud:*** This is a infrastructure which is available to only a specific group and only that group is able to acess it [1].

***c) Community cloud:*** This is a cloud infrastructure which is available for more than one organization means it can be shared between two organizations whose cloud requirements such as security policy etc are same.[1].

***d) Hybrid cloud:*** This is a infrastructure which is a mixture of public and private cloud[1].

#### *b. Service Models:*

Cloud computing can be classified based on the services it offers.

***a) Infrastructure as a service:*** This is a infrastructure in which the network and computational resources are provided to the customers as a service and the users can run any operating system and software on the infrastructure[1]

***b) Platform as s service:*** In this the platform is provided by the cloud provider on which web base applications have to run [1].

***c) Software as a service:*** It is a model in which application is provided to the customer .and the user can acess these services and softwares. When the software isnot available on cloud means when software is offline the user can't acess it[1].

#### *c. Cloud Characteristics:*

***a) On demand service:*** In this the Cloud act as a Service Pool from which the end user acess the resources

whenever required by paying the amount of that resources[1].

***b) Ubiquitous network access:*** In this the Cloud Provide Services to everywhere through mobile phones laptops etc[1].

***c) Easy use:*** In this the cloud providers provide internet based interface which is better than application based so that the end users can easily use it[1].

***d) Business model:*** The cloud can be say that the business model because the user can acess any resource from the cloud whenever required by paying its payement[1].

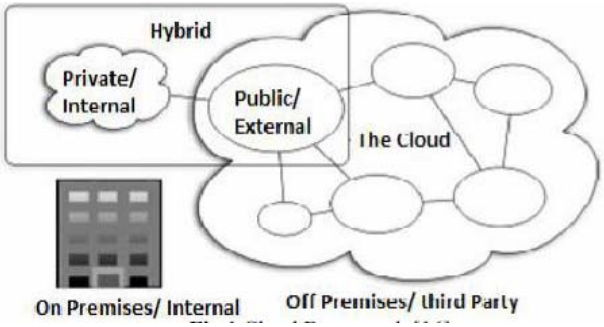


Figure. 1 Cloud Framework [1]

### *B. Related Work:*

"Cloud Computing is a recent term Which is used in almost every field . Cloud Computing Shared the information on data centres from which the different persons of same field come in contact with particular organization or individual for eg we can share the report of the particular patient on Cloud then with the help of this different doctors can see that report and give their views. Cloud Computing is used in many fields like it is used in Military, Entertainment, Buisness etc .We can improve our business with the help of Cloud [2].Cloud Computing is an important and Modern technique which is used in almost every field.Cloud Computing have Various data centres on Which the information is Shared.Cloud Computing Shared its information geographically on these Data centres.To design a secure data acess to Cloud is the major issue.But this Paper proposed a secure data acess Scheme based on identity based encryption and biometric authentication for cloud computing . In this we deal with the two Schemes first We have to deal with Security acess to the Cloud then we have to deal with data integrity acess to the Cloud.

### *C. Proposed Work:*

One of the critical aspect of cloud computing is the secure management of the resources that are associated with cloud services. One of the main tasks of secure management is cryptographic operations. Hence, while self-configurable resources, elastic capabilities and ubiquitous computing isprovided by cloud services at a lower cost, they also entail performing several cryptographic operations for the following:

a) To provide secure storage of data that is processed by those services.

b) To provide secure interaction of the cloud consumer with various services.

The above functions can increase the complexity of the key management system (KMS) required to support the cryptographic operations for these functions for the above because differences in control and ownership of underlying infrastructures on which the resources and KMS are located. Solution to the security issues

In order to manage the encryption keys securely, enterprises need to employ encryption in their cloud environment, while maintaining secure off-site storage of their encryption keys.

Encryption keys should never be stored in the same place as encrypted data. The keys used for encrypting sensitive customer data should be managed effectively by periodic key rotation, and re-encryption of data with new keys.

Employees should be not be given more access than what is needed to complete their tasks.

### *D. Experimental ImplementationRC4*

RC5 is an fast symmetric block cipher. A symmetric block cipher is a cipher that uses the same key for encryption and decryption as shown in the figure below. The plaintext and cipher text are fixed-length bit sequences, that is why it is a block cipher

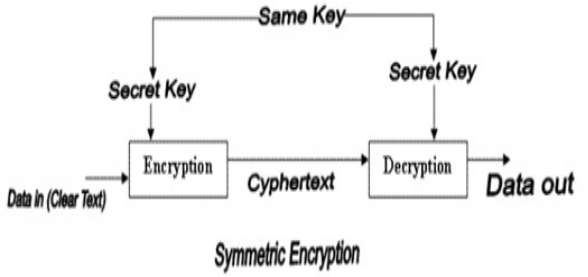


Figure: 2

### *E. Important Parameters:-*

a. w It specifies the variable word size in bits. Thought the algorithm is designed for any arbitrary length of the word size, that is an integer greater than zero, but all the choices need not necessarily serve the purpose of the required security wherever the algorithm is implemented. Therefore, only the choices like 16, 32 and 64 are allowed for RC5 algorithm and the suggested choice is 32. RC5 algorithm takes two word input plaintext, making it a 64-bit plaintext input and gives a two word output cipher text, making it a 64-bit ciphertext output.

b. r It specifies the variable number of rounds. The number of rounds acts as a trade of between high speed and high security. For the same reasons as specified in the parameter 'w', the suggested value for the number of rounds is 12. The allowed values for the number of rounds are 0, 1, .... 255.

c. b It is the variable length secret cryptographic key. 'b' specifies the number of bytes in the secret key K. For the same reasons as specified in the parameter 'w', the suggested value for 'b' is 16, while the allowable values are from 0 - 255.

d. K It is the b-byte secret key array : K[0], K[1], ...,K[b-1]. RC5 cannot be secure for all possible values of the number of rounds 'r' and length of the secret cryptographic key 'b'. That means that if the number of round(s) is zero, it implies that there is no security. If the number of round(s) is one, it will provide very less security and as a matter of fact, it can be easily broken.

Similarly, if 'b' is zero, then there is no key, therefore there is no security. On the other hand if the maximum allowable values are used for these parameters then this might be an overkill. Therefore, the nominal choice that is proposed is :- w - 32 r - 12 k - 16 The notation to write all the parameters for the RC5 algorithm is RC5-32/12/16. Some important notations and the RC5 Primitive Operations:- There are three primitive operations(and their inverses):- 1.) Two's complement addition of words, that is done modulo 2w . It is denoted as a '+' symbol and the inverse operation is subtraction and it is denoted by '-'. 2.) Bit-wise exclusive OR of words. It is denoted by the ⊕ symbol. 3.) A left rotation of words, that is the cyclic rotation of a particular word x left by y bits. It is denoted as x<<>>y. The important point to note is that the rotations are "rotations by variable amount" and that amount is not fixed. We also have the knowledge that on modern microprocessors, a variable rotation takes constant-time, so the time is independent of the rotation amount. There are no other non-linear operations in RC5. Therefore, the strength heavily relies on the data dependent rotations. Let's have a look at the RC5 algorithm, that is divided into three parts:-

a) Key Expansion
b) Encryption Algorithm
c) Decryption Algorithm

***a) Key Expansion*** - Let's see what are requirements of the key expansion. There is an expanded key table array S that will contain the random binary words that will be used in the encryption and decryption later on. The size of this table is dependent upon the number of rounds 'r' mentioned above. The size of this table is given by, t = 2 (r +1)where

,t - is the size of the table S.
r the number of rounds in the RC5 algorithm

Note:-The S table array should not be mistaken with the S-box concept in the DES algorithm. Entries in the S table array are used sequentially, one at a time.

The random binary words that are required to fill this array are derived from the key array K. We start with two magic constants:-

These are two word-sized binary constants
Pw = Odd((e - 2) 2w )
Qw = Odd((φ – 1) 2w )
where, e = 2.718281828459… (base of natural logarithms)
Φ = 1.618033988749… (golden ratio),
Odd(x) = odd integer nearest to x
For w = 16 and 32 in hexadecimal form
P16 = b7e1
Q16 = 9e37
P32 = b7e15163
Q32 = 9e3779b9

Step 1: Converting the Secret Key from Bytes to Words:-
The secret key array K is copied into another array L, where the size of the array L is
c = ceiling(b/u) words.
where,
u = w/8 is the number of bytes/word.

u consecutive key bytes of K fill up each successive word in L, low-order byte to high-order byte and the remaining positions are zeroed.

When b=c=0, then c becomes 1 and L[0] is set to zero.

Assuming all the bytes of the key are unsigned and the array L is initially zeroed, the following pseudo code copies the secret key from bytes to words on the little endian machines.

$$c = \lceil \max(b,1)/u \rceil$$
$$\text{for } i = b-1 \text{ downto } 0 \text{ do}$$
$$L[i/u] = (L[i/u] \lll 8) + K[i];$$

Step 2: Initializing the Array S:- The array S is initialized with the help of the magic constants. This step is key independent. This initialization of array S is done using an arithmetic progression modulo 2w determined by the magic constants.
Following is the pseudo code to do the same:-

$$S[0] = P_w;$$
$$\text{for } i = 1 \text{ to } t-1 \text{ do}$$
$$S[i] = S[i-1] + Q_w;$$

Step 3: Mixing in the Secret Key The final step is mixing of the secret key which can be done by the following pseudo code:-

$$i = j = 0;$$
$$A = B = 0;$$
$$\text{do } 3 * \max(t,c) \text{ times:}$$
$$A = S[i] = (S[i] + A + B) \lll 3;$$
$$B = L[j] = (L[j] + A + B) \lll (A + B);$$
$$i = (i+1) \bmod (t);$$
$$j = (j+1) \bmod (c);$$

Encryption Algorithm The two w-bit words inputs are denoted as A and B.
A = A + S[0];
B = B + S[1];
for i = 1 to r do
A = (( A⊕ B ) <<< B ) + S[ 2 * i ];
B = (( B⊕ A) <<< A ) + S[ 2 * i + 1];

The output are in the registers A and B. Work is done on both A and B, unlike DES, where only half input is updated ina particular

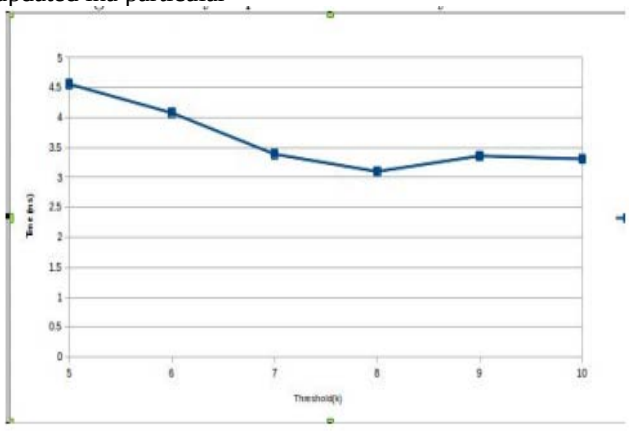


Figure: 3

Round. Next is the diagram, which demonstrates the above algorithm and another diagram following that demonstrate the encryption implementation on the hardware. The second diagram is more helpful in understanding the encryption.

It includes the time to encrypt the file as requested by the client.It is the time between the points when user requests the cloud system to upload the file and the time when the tasks of encryption and generating key shares actually finishes and the encrypted file is actually stored in the cloud data

## II. CONCLUSION

We proposed algorithm for cloud security.

With this algorithm a encryption technique is used for creating random script which are converted with cypher text and encryption technique are followed for better data security. Further various encryption techniques can be used for data encryption technique in future work

## III. REFERENCES

[1]. Aparjita Sidhu, Rajiv Mahajan, "Enhancing Security in Cloud Computing Structure by Hybrid Encryption". International Journal of Recent Scientific Research, Vol.5, Issue.1, pp.128-132, January 2014.

[2]. Manoj Chopra, Jai Mungi, Kulbhushan Chopra, "A Survey on Use of Cloud Computing in Various Fields". IJSETR, Vol.2, Issue.2, February 2013.

[3]. Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security". IJETAE, Vol.3, Issue.12, December 2013.

[4]. Khushdeep Kaur 1, Er. Seema 2, "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices". International Journal of Engineering Research and Applications, Vol.2, Issue.5, September-October 2012, pp.914-917.

[5]. Cheng Hongbing, Rong Chunming, "Identify Based Encryption and Biometric Authentication Scheme for Secure Data Access in Cloud Computing". Chinese Journal of Electronics, Vol.21, No.2, Apr. 2012.

[6]. Anjum Asma, Mousmi Ajay Chaurasia and Hala Mokhtar, "Cloud Computing Security Issues". IJAIEM, VOL.1, Issue.2, October 2012.

[7]. Farhad Soleimanian Gharehchopogh, Sajjad Hashemi, "Security Challenges in Cloud computing with More Emphasis on Trust and Privacy". International Journal of Scientific & Technology Research, Vol.1, Issue 6, July 2012.

**Short Bio Data for the Authors**

**Harmanjeet Kaur** She obtained her B.Tech (computer science&engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Cloud Computingand Security threat in cloud computing

**Ms. Neha Bhardwaj** is working as an assist. professor in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. She obtained her B.Tech (computer science engineering) from Amritsar college of Engineering and Technology, Manawala, Amritsar, Punjab, India, M.Tech (computer science & engineering) from Amritsar college of Engineering and Technology, Manawala, Amritsar, Punjab, India.