Analysis of Rc5 to enhance source and Security in cloud computing

Harmanjeet Kaur, Neha

***Abstract*— Cloud computing is a globalized concept and there are no borders within the cloud. Computers used to process and store user data can be located anywhere on the globe, depending on where the capacities that are required are available in the global computer networks used for cloud computing. Because of the attractive features of cloud computing many organizations are using cloud storage for storing their critical information. The data can be stored remotely in the cloud by the users and can be accessed using thin clients as and when required. One of the major issue in cloud today is data security in cloud computing. Storage of data in the cloud can be risky because of use of Internet by cloud based services which means less control over the stored data. One of the major concern in cloud is how do we grab all the benefits of the cloud while maintaining security controls over the organizations assets. Our aim is to propose a more reliable, decentralized light weight key management technique for cloud systems which provides more efficient data security and key management in cloud systems. Our proposed technique provides better security against byzantine failure, server colluding and data modification attacks.**

***Index Terms*— 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 application.The term cloud has been found from compicated infrastructure [3].Cloud Computing is the newest technology in field of Information technlogy .Because of is new technology It is difficult for both the Producer and consumer to use it[8]. Therefore in recent days cloud computing has become a major challenging issue [1]. The issue of using Cloud is most Challenging Thus Most of users avoid to use it[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 applied at present. But these models have failed to solve most of the security threats. Moreover for E-commerce anddifferent types of online businesses high capacity security modelsare implied in cloud computing fields. Security models that aredeveloped and currently used in the cloud computing environments are mainly used for providing security for a file andnot for the communication system. Moreover present securitymodels are sometimes uses secured channel for communication.But this is not cost effective process. Some models attempt ondiscussing about all of these but are completely dependent on userapproach. [1]. As encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we are focusing on security enhancing by enhancing the level of encryption in network [5].

Various algorithms have been used to provide message security. It is good practice to encrypt the actual message to be transmittedusing a Symmetric key algorithm with better computational speedfor cloud environment. Firstly Advanced Encryption Standard isused in which keys are generated randomly by the system. AES isa block cipher with a block length of 128 bits and also allows forthree different key lengths 128, 192 or 256 bits. AES has differentrounds which are performed for each block. Except for the lastround in each case all other rounds are identical. In the processingsteps used in single round 128-bit block is divided into 4 by 4matrixes of bytes. The 4 by 4 matrix of bytes is referred to as thestate array [1]. The steps performed for each block are same forencryption and decryption but the order in which they areperformed is different. Secondly message digest hash function issued which is a cryptographic hash function with a 128-bit hash value.This hash function is expressed as a 32-digit hexadecimalnumber. This algorithm outputs a particular length string whichcan be used in password handling. for example the messagecontent is hello how are you. Now each word is calculated and its digest is produced. Let its digest is 89 so 89 is send during thecommunication. Message digest operates with following steps:

- Append Padding Bits
- Append Length
- Initialize MD buffer
- Process message in 16-word blocks
- Output

The main purpose of message digest hashing algorithm is that this method is a one way system and unbreakable. Therefore itwill be difficult for an unauthorized or unknown party to retrievethe password for a selected user even if gained access to thesystem [1].

II. RELATED WORK

Aparjita [1] said that Modern communication is containing different types of networks depending on the behavior of users. Cloud network and services are one of the mostly used networks. Security in the cloud service architecture is always a big concern for the vendor as well as users. In this paper

Harmanjeet Kaur, Student, M.Tech (CSE), PTU
Neha, Assistant Professor, PTU

distributed cloud service architecture is considered which is used as network detection system for outer attacks to the cloud architecture. Outer attacks can be prevented by security services such as McAfee, Imperva etc. but insider attacks are very difficult to detect and to avoid them, different resources consuming processes are considered. So to provide solution for security without spending many resources, encryption of messages is a good option. Hash function encryption is easy and light encryption process which will challenge the odds and can be suitable for cloud computing structures.

Anjum [5] state that Cloud Computing is the latest paradigm that involves delivering hosted services over the Internet, based on pay-as-you-go approach. Cloud computing provides number of benefits out of which economic benefit is main benefit. With the lots of benefits some challenges are there to be solved and out of which security is a major challenge. Cloud security issue is a critical issue and because of this users are hesitating to use the clouds. In this paper we surveyed the cloud computing security issues. Our main contribution is to classify the issues according to the different service models and to provide some directions for solutions. Enough or adequate security can be achieved by solving these issues.

Farhad Soleimanian [7] state that Cloud computing is the newest technologies in IT field which causes some worries for consumers and its producers due to its novelty. Looking at its literature, we can see the privacy and security aspects and trust are the main concerns. It creates an important hindrance for using by users. So we decided to evaluate some factors such as security for the acceptance of cloud computing. In this paper, we highlighted envision about security emphasizing for the maintenance of privacy and trust in accepting the cloud computing. As a result, we are proposed new recommendations for improving security, decreasing risks, increasing trust and maintaining privacy which they are necessary to adopt cloud computing.

Venkata Narasimha Inukollu [8] *state that security issues for cloud computing, Big data, Map Reduce and Hadoop* environment. The main focus is on security issues in cloud computing that are associated with big data. Big data applications are a great benefit to organizations, business, companies and many large scale and small scale industries.We also discuss various possible solutions for the issues in cloud computing security and Hadoop. Cloud computing security is developing at a rapid pace which includes computer security, network security, information security, and data privacy. Cloud computing plays a very vital role in protecting data, applications and the related infrastructure with the help of policies, technologies, controls, and big data tools**.** Moreover, cloud computing, big data and its applications, advantages are likely to represent the most promising new frontiers in science.

III. Results Analysis

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:

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

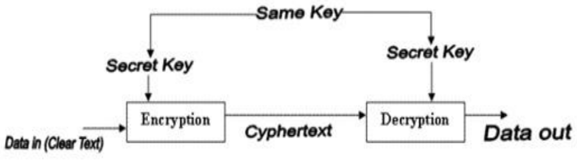
In order to manage the encryption keys securely, enterprises need to employ encryption in their cloud environment, while maintaining secure off-site storage of their encryption keys.

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.

Experimental ImplementationRC5

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



Symmetric Encryption

Important Parameters:-

1.) 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.

2.) 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.

3.) 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.

4.) 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:-

1.) Key Expansion
2.) Encryption Algorithm
3.) Decryption Algorithm

1.) 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.

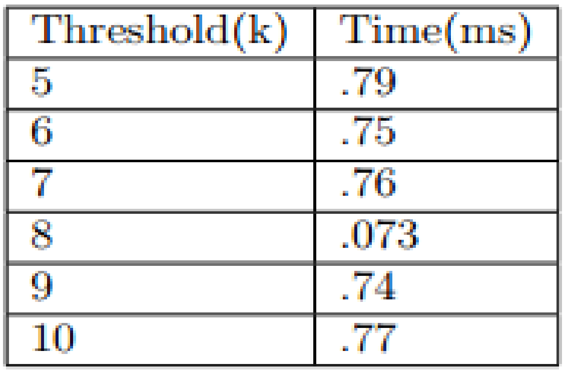
Assuming all the bytes of the key are unsigned and the array L is initially zeroed, the following pseudo code copies the secret key from bytes to words on the little endian machines.

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.

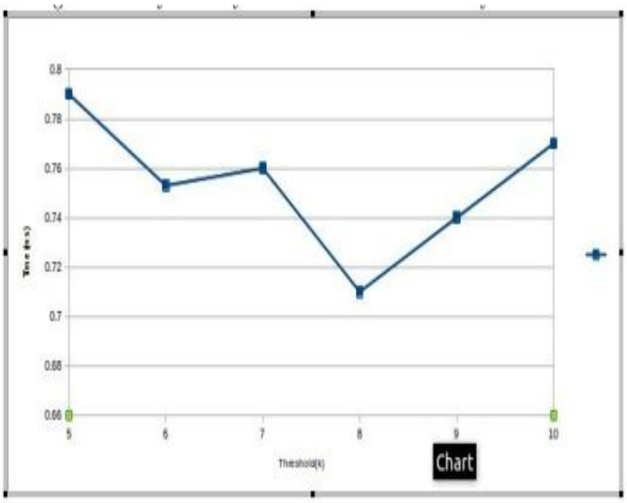
Step 3: Mixing in the Secret Key The final step is mixing of the secret key

Figure 2 shows the comparison graph of file upload and download scheme. The efficiency of our proposed Rc5 algorithm scheme achieves the highest performance with lesser time while the other schemes take more time consumption. As it is more time-consuming for the adversary to capture the sink than the source, the safety period of the sink location privacy is also larger than that of the source location privacy.

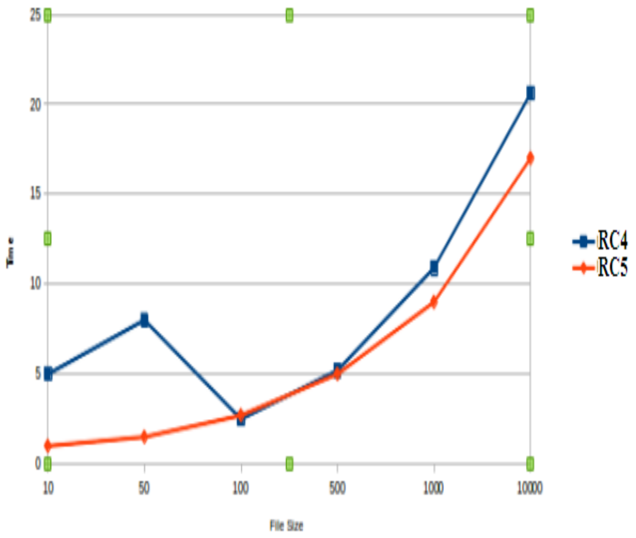
. Next is the diagram, which demonstrates the above algorithm and another diagram following that demonstrate the encryption implementation on the hardware. The second diagram is more helpful in understanding the encryption.

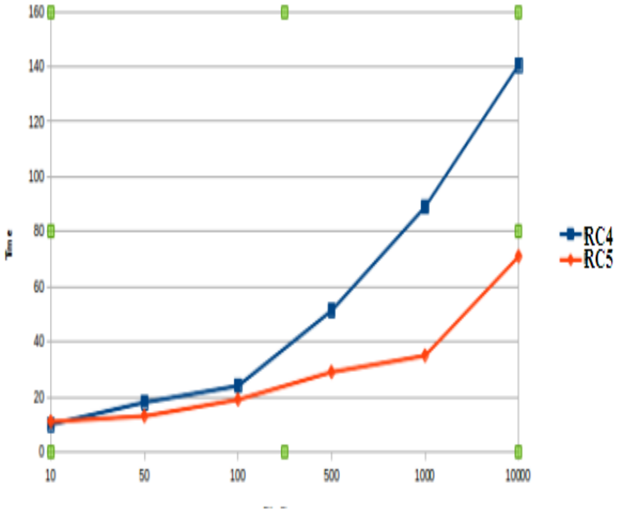


Threshold(k)	Time(ms)
5	.79
6	.75
7	.76
8	.073
9	.74
10	.77



secondary key, merge the master key and the secondary key and time to decrypt the input file. It is the time between the two points when the user makes a request to download a file and user actually receives his file. Figure shows the time taken for file downloading for different file sizes.





.

IV. CONCLUSION

In this chapter we have proposed a system which removes the drawbacks of some of the existing cloud systems. New modules are added to the existing system to improve the reliability and security of the existing cloud systems that use symmetric key encryption techniques to ensure data security. Key management is the toughest part to manage in cryptosystems. In the cloud platform, there is always a possibility of insider attack or outsider attack. Keys can be accessed or stolen by employees without the knowledge of end users. Our aim is to provide secrecy to the data as well as keys that are stored in cloud systems. Our proposed technique provides better data security and key management in cloud systems. This technique also provides better security against failure, server and data modification attacks.

In future, this work can be extended to use some other secret sharing schemes which are more efficient so that the performance of proposed system can be further improved. In addition to this, the proposed technique can be extended to work with asymmetric encryption algorithms.

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.

[8] Venkata Narasimha Inukollu, Sailaja Arsi and Srinivasa Rao Ravuri, “SECURITY ISSUES ASSOCIATED WITH BIG DATA IN CLOUD COMPUTING”. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014.