Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhanced Encryption Algorithm for Information Security by Random Key Selection in a Distribution Based Cloud Network

Chandrashekar S, Shince T Thomas

M. Tech, Department of Computer Science and Engineering, BNM Institute of Technology, Bangalore, Karnataka, India

Abstract— In this paper, we proposed our new symmetric key encryption calculation with decreased space many-sided quality (AM Encryption Algorithm-NEA). As indicated by circle encryption hypothesis an encryption system ought to utilize not exactly or equivalent to the extent of the first document size. There are two most imperative parameters or attributes of calculation time and space. A calculation ought to require least time to perform their capacity and ought to have least space multifaceted nature (space many-sided quality regarding storage room after the encryption or the storage room required to store figure content). Diverse sorts of calculation has been outlined some of them gives better security yet the space intricacy of all current calculation is high. Thus, we proposed another cryptographic calculation taking into account symmetric key stream figure that furnishes better security with least space unpredictability. This calculation is not same as past stream figure calculation (the most ordinarily utilized RC4) it has some new components, for example, Random Key Selection with transposition that gives better security.

Keywords— Space complexity, Cryptography Algorithm, Symmetric key, Network security, Random key generation, AES, Random key selection.

I. INTRODUCTION

Encryption is critical method to give secrecy while transmitting information over remote medium, since remote mediums are an open channel where data can without much of a stretch got to or changed by unapproved people groups. On the remote channel there is no any ensure that the information can't be gotten to by someone else on remote channel, so security is huge test to ensure information over remote system. It might be extremely perilous when any individual needs to send their classified information over the system, for example, Bank_Statement, Bank_Transaction or some other vital data. a man is sending some classified information starting with one point then onto the next point then those data ought not be gotten to by unapproved individual the data ought to be shielded from programmer. In view of security issue today arrange security and cryptography is a major exploration zone where the general population dependably attempt to plan some new calculation in a steady progression to ensure information against unapproved individuals. Cryptography calculation for the most part separated into two sections (i) Symmetric Key Algorithm-In this method a solitary key is utilized by sender and in addition recipient [1]. Symmetric key gives encryption quicker however here and there it is anything but difficult to break the key of this calculation as a result of straightforward key administration. There are two sorts of symmetric key encryption calculation, stream figure and square figure and (ii) Asymmetric key Algorithm-it is otherwise called open key cryptography calculation it utilizes two unique sorts of key for figure and translating. Open key cryptography gives more security in contrast with symmetric key yet it is slower than symmetric key. Out in the open key cryptography the general population key is known by everybody while the private key is known by the approved individuals and it must be kept mystery, open key and private key both are numerically interrelated to each other. These days burglary of information over system expanding at fast so there are distinctive sorts of encryption calculation has been created like AES, DES, TDES, Blowfish RC6 and so on and all these calculation has its own benefits and negative marks. Because of absence of channel limit and to spare circle space it is vital that the encryption method ought not to require space more than the span of plain content [2]. For this, numerous creators have proposed their thought to decrease the span of encoded information however all has some hindrance and nobody has been effectively executed. In this paper, we proposed another symmetric key encryption calculation that gives better security and requires least space in contrast with its related calculations.

II. RELATED WORK

Security gives a systems administration foundation to connecting server farms to mists and an enhanced type of live. Security and Space both are imperative issues in light of robbery and clog on system. In [3], creator demonstrates that how much space is required by symmetric key encryption calculation what's more, gave their thought to decrease the measure of scrambled information; creator says that we can perform just XOR operation so it is not more secure procedure. In [7], creators have proposed an encryption calculation utilizing wavelets change strategy for picture encryption. Archana.V.Nair.S [8] has proposed an encryption calculation utilizing number juggling coding yet creator says that utilizing number juggling coding there is issue in unscrambling it is difficult to discover exact character when digits are adjusted. Numerous creators have gave their thought that that we can utilize number-crunching coding to lessen the measure of scrambled information, on the off chance that we utilize math coding then it decreases the span of figure content however it makes calculation to moderate and there is have to utilize additional memory space and the execution would be moderate. Existing calculations, for example, AES, DES, TDES, RC4, RC6 and Blowfish require some additional space for scrambled information.

III. PROPOSED WORK

In this section we discussed a new encryption algorithm with reduces space complexity and provides high security. This is a symmetric key stream cipher algorithm and this is not similar to other symmetric key encryption algorithm. There are two major operations are performed in proposed algorithm Random Key Generation and Random Key election which makes this algorithm secure. In previous stream cipher algorithm RC4 where a random bit is added in cipher text for security purpose that takes extra space but in this algorithm we enhance security using random key generation and random key selection and do not require any extra space for encrypted data. This algorithm performs variable processing rounds of encryption, the number of rounds depends on the length of the key and in each round we are generating random key and then encrypt data using random key. Using random key generation this algorithm provides better security because it is impossible to predict the new key in each round, after performing Random key generation function proposed algorithm has two different keys. Now in random key selection function it is decided that which key should use for encryption. There three main processes in AMEA (A) Random Key Generation (B) Random Key Selection and (C) Transposition.

A. Random key generation

NEA performs many rounds, in each round random key generation generates random key from the previous key by performing some mathematical calculation. After generating random key this algorithm contains two different key the first one is previous key and second is the newly generated key. The idea behind the generating of two different key is that if any one try to crack the key then it is impossible to predict the key in each round. Random key is generated by using the ASCII value and the position of each character in the key then apply random function with some operation on matrix. Briefly describe in the example.

B. Random key selection

AM Encryption Algorithm contains two different keys after random key generation function. Now the main task of RKS is to select any one key between two keys as key1 and key2. It takes two keys as an input and converts them into equivalent binary, after converting find the LSB of both keys and compare their LSB. If LSB of both keys are equal then select key1 otherwise select key2 to perform encryption. RKS also provides better security against attacks because attacker does not know which key is used for encryption. This function is performed in each round.

C. Transposition of key

Transposition is a function or method through which the character of the key is replaced by another character of the key. The character is shifted based on regular system. When the key is selected by random key selection function then algorithm applies transposition function with the key. To transpose the key, algorithm first finds the random number and then calculate sum of total of random number. When sum is calculated then according to the number in summation algorithm replace the character of the key. For Example, if the value of sum is “3214” and the key value is “adsetguim” then character ‘a’ is interchanged by the character on (3-1) = 2nd position in the key, ‘d’ is interchanged by the character on (2-1)=1st position in the key, after 4th character repeat with the same value of summation.

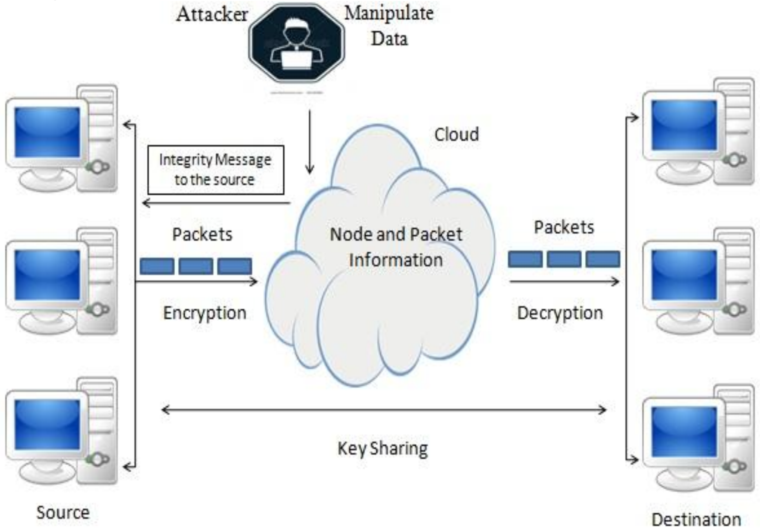

Fig. 1 Encryption and decryption process of packets

The above architecture explains the process of encryption of packets and it stores the information in cloud, after it decrypts the packets to get exact information to the destination.

IV. PROPOSED ALGORITHM

A. The Algorithm for encryption and decryption

```
Step 1: read plaintext
Step 2: Enter key as key1 and initialize Round as 0.
Step 3: Find the length of the key L.
Step 4: Call transpose function // Algorithm defined below
Step 5: while R<= L/2
    ➢ Obtain new key from random_key_generation function as key2.
    ➢ Call random_key_selection (key1, key2)
    ➢ Now key= selected key from random key selection
    ➢ Now call transpose function(key)
    ➢ Obtain final key to encrypt/ decrypt

Step 6: perform Exclusive-or operation with transposed key and plaintext/cipher
Step 7: R=R+1
Step 8: Stop.
```

B. Algorithm for random key generation

```
Step 1: read the key sent as a parameter (Key1)
Step 2: Find the length of key1
Step 3: Now reverse key1 by using reverse function, new reversed key is termed as in rev_key.
Step 4: Convert each character of key1 in its equivalent ASCII code.
Step 5: Calculate total number of random_value = L, Rand(Max)
Max= ΣASCII * Sequence of each character.
Step 6: Find the sum of total random_value
Step 7: Find mod of sum_of_random, M= Mod(sum_of_random, l)
Step 8: Apply matrix on key1 and rev_key
Step 9; Add 'M' to each bit of matrix _key1.
Step10: Apply XOR operation with matrix_rev_key and matrix_key1.
Step11: Obtained new matrix as new_matrix.
Step12: Convert binary of new_matrix to change into character and stored in new matrix (Key2).
Step13: return two keys (key1, key2)
```

C. Algorithm for random key selection

```
Step 1: Read two keys from random key generation
Step 2: Convert each character of key1 and key2 into its equivalent ASCII
Step 3: multiply each ASCII with the value 'M' (M obtained in RKG)
Step 4: convert into binary.
Step 5: Find the Least Significant Bit of both keys as LSB1 and LSB2
Step 6: If LSB1= = LSB2
    ➢ Select key1 and
    ➢ Call transpose function (key1) //calling transpose function with key1
Else
    ➢ Select key2
    ➢ Call transpose function (key2) //calling transpose function with key2
Step 7: Stop.
```

D. Algorithm for Transposition

```
Step 1: Read selected key as key1
Step 2: Read sum= sum_of_random
Step 3: Read each character of sum individually
Step 4: The character of the key1 is interchanged with the character indexed on the (value-1) of corresponding number in sum.
Step 5: Increase the index of key1 and sum by 1.
Step 6: Repeat the step 4 and 5 until the last index of the key
Step 7: finally obtain the key to encrypt and decrypt.
Step 8: Stop.
```

V. EXPERIMENTAL RESULTS

This section shows the result given by AM- Encryption Algorithm and also shows how much space is required for cipher text in comparison to another encryption technique.

Table I. Experimental Result of NEA

Sl. No.	*Size of plaintext*	*Size of Encrypted file*	*Size of Decrypted file*
1.	180 KB	180 KB	180 KB
2.	230 KB	230 KB	230 KB
3.	490 KB	490 KB	490 KB
4.	1890 KB	1890 KB	1890 KB

Table II. Comparision of Proposed Encryption Algorithm with Most Common Encryption Algorithm

Sl. No.	*Encryption Algorithms*	*Size of plaintext*	*Size of Encrypted file*	*Size of Decrypted file*
1.	DES	260 KB	376 KB	260 KB
2.	TDES	260 KB	720 KB	260 KB
3.	AES	260 KB	1034 KB	260 KB
4.	NEA	260 KB	260 KB	260 KB

VI. CONCLUSION AND FUTURE SCOPE

CloudNet security gives a systems administration foundation to connecting server farms to mists and an enhanced type of live. Security and Space both are imperative issues in light of robbery and clog on system. In [3], creator demonstrates that how much space is required by symmetric key encryption calculation what's more, gave their thought to decrease the measure of scrambled information; creator says that we can perform just XOR operation so it is not more secure procedure. In [7], creators have proposed an encryption calculation utilizing wavelets change strategy for picture encryption. Archana.V.Nair.S [8] has proposed an encryption calculation utilizing number juggling coding yet creator says that utilizing number juggling coding there is issue in unscrambling it is difficult to discover exact character when digits are adjusted. Numerous creators have gave their thought that that we can utilize number-crunching coding to lessen the measure of scrambled information, on the off chance that we utilize math coding then it decreases the span of figure content however it makes calculation to moderate and there is have to utilize additional memory space and the execution would be moderate. Existing calculations, for example, AES, DES, TDES, RC4, RC6 and Blowfish require some additional space for scrambled information.

ACKNOWLEDGMENT

I would like to thank to my parents, friends, Proof Readers and thanks to my respected guide for their support in every step. He always guided and motivated me to complete this research paper.

REFERENCES

[1] M. A. Tiwari, C. Parakash and AK. Mandal, "*Performance Evaluation of Cryptographic Algorithms: DES and AES*", 2012 IEEE Student's Conference on Electrical, Electronics and Computer Science.

[2] http://en.wikipedia.org/wiki/Disk_encryption_theory accessed on 24th April 2014.

[3] V. Singh and S. K. Dubey, "*Analyzing Space Complexity Of Various Encryption Algorithms*", International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 1, January- February (2013).

[4] A. Ramesh and Dr. A. Suruliandi, "*Performance Analysis of Encryption Algorithms for Information Security*", 2013 International Conference on Circuits, Power and Computing Technologies, IEEE, 2013.

[5] Amit Pande, Joseph Zambreno and Prasant Mohapatra, "*Joint V ideo Compression and Encryption using Arithmetic Coding and Chaos*", 978-1-4244-7932-0/10, IEEE,2010.

[6] William Stallings, i 5th Edition-2010, p.p 66-174.

[7] Nidhi Sethi and Deepika Sharma, "*A Novel Method Of Image Encryption Using Logistic Mapping*", International Journal of Computer Science Engineering, Vol. 1 No.02 November 2012.

[8] Archana.V.Nair.S, G.Kharmega Sundararaj and T. Sudarson Rama Perumal, "*Simultaneous Compression and Encryption using Arithmetic Coding with Randomized bits*", International Journal of Computer Technology and Electronics Engineering (IJCTEE), Volume 2, Issue 2, April 2012.

[9] Dr. R. Umarani, G. Ramesh and E. Thambiraja, "*A Survey on Various Most Common Encryption Techniques*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.

[10] Md Asif Mushtaque and Mr. Khushal Singh, "*Feasibility Evaluation of Symmetric Key Encryption Techniques for Wireless Channel and Disk Storage*", IJRASET, Vol. 2 Issue V, May 2014.

[11] Tingyuan Nie, Yansheng Li and Chuanwang Song, "*Performance Evaluation for CAST and RC5 Encryption Algorithms*", International Conference on Computing, Control and Industrial Engineering, IEEE, 2010.

[12] Anjali Patil, Rajeshwari Goudar, "*A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices*", International Journal Of Scientific & Technology Research Volume 2, Issue 8, August 2013.

[13] Md Asif Mushtaque, Harsh Dhiman, "*Implementation of New Encryption Algorithm with Random Key Selection and Minimum Space Complexity*", International Conference on Advances in Computer Engineering and Applications, 2015