ISSN: 2321-7782 (Online)
Volume 3, Issue 6, June 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Design & Analysis (Computing power, Complexity, Security) of new encryption-decryption algorithm for enhanced cloud security

Arun Singh Chouhan[1]
Associate Professor, Department of Computer Science
Vyas Institute of Engineering & Technology
Jodhpur - India

Shalini Agarwal[2]
M.Tech Student, Dept. of Computer Science
Chandravati Education Charitable Trust Group Of Institute
Bharatpur - India

Abstract: ***In this computing era the cloud computing technology and services are the most promising & valuable model for compute, storage, on demand services and software. It provides user to complete development environment, virtualization, allocation and reallocation of storage resources and sharable services like "as-a-services". The cloud network security issue is main concern because the data send and receive between the user and cloud service provider totally depends upon the data centres and these data centres are managed by third party, so it is required to encryption and decryption mechanism or secure algorithm on that data transmission. We design an algorithm that enhanced the cloud based systems and network security that will base on symmetric cryptographic algorithm.***

Keywords: Key management, Symmetric Algorithm, Cloud models, Encryption and Decryption.

I. INTRODUCTION

In this computing era the cloud computing technology and services are the most promising & valuable model for compute, storage, on demand services and software. It provides user to complete development environment, virtualization, allocation and reallocation of storage resources and sharable services like "as-a-services". The cloud network security issue is main concern because the data send and receive between the user and cloud service provider totally depends upon the data centers and these data centers are managed by third party, so it is required to encryption and decryption mechanism or secure algorithm on that data transmission. We design an algorithm that enhanced the cloud based systems and network security that will base on symmetric cryptographic algorithm. [1] Cloud computing combines the data-sharing model and service statistical model. From a technical point of view, cloud computing has the following three basic characteristics. Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server architecture. Through the strong performance, the traditional mainframe's prices are also very expensive. Collaborative development of the underlying services and the applications is to achieve maximum resource utilization. By this way, application's construction is improved. But for traditional computing model, applications to be complete dependent on the underlying service. The redundant problem among multiple low-cost servers is solved by the software method. Because of using a large number of low-cost servers, Failure between nodes cannot be ignored, so the issue of fault tolerance among nodes should be taken into account, when designing software.[2] Our research works towards design a new cryptosystem follows the sequence of steps identifies the methodology adopted in this work.

II. PRESENT WORK

In our present work an algorithm is developed. The algorithm uses a matrix key which on multiplication with a quaternary vector and applying a sign function on the product generates a sequence. This sequence will be used to generate three different models of substitution technique. Thus the algorithm is considered to be a substitution algorithm which uses a single key to be

shared by both the sender and receiver, and the cipher processes the input element continuously, producing output one element at a time. The new encryption algorithm is based on the concept of Poly alphabet cipher which is an improvement over mono alphabet.

III. Algorithm for Generating the Sequence

STEP# 1. Consider the sequence for 0 to N values where N is a positive integer.

STEP#2. Convert each element of the sequence into Quaternary form of a given digit number.

STEP#3. Represent the values of STEP#2 in a matrix form of (n+1) * (digit number).

STEP#4. Subtract 1 from each element of the matrix specified in STEP#3.

STEP#5. Consider a random matrix key of size (digit number*digit number).

STEP#6. Multiply the output of STEP#4 with the output of STEP#5.

STEP#7. Convert all positive values of matrix to 1, negative values to -1 and zero by 0.

STEP#8. Add 1 to each element of output of STEP#7.

STEP#9. Convert Quaternary values of STEP#8 into decimal form. A sequence is generated.

IV. Computing Power Analysis of Algorithm

Total number of computations considered in the given model for converting plain text to cipher text.

Computation one: Converting n=0:255 to Quaternary vector. Let it be QVR.

Computation two: Calculating QVR-1 and storing it in QVR.

Computation three: Multiplying QVR with the key considered.

Computation four: Applying sign function on the product. Store it in QVR.

Computation five: Calculating QVR+1.

Computation six: Converting output Quaternary vector to integer form.

Let this be SEQ, the sequence generated.

Computation seven: Converting plain text to ASCII.

Computation eight: Adding ASCII value of plain text to sequence generated.

Computation nine: Applying mod function on the output.

Computation ten: Converting the output to characters of the alphabet to get cipher text.

Thus the total number of computations in the first proposed model is 10.

Computation overhead (Computing Power) for a 16 character key

1st computation: 256 calculations,

2nd computation: 256 calculations. Key considered: character key,

3rd computation: 256*16 calculations,

4th computation: 256 calculations,

5th computation: 256 calculations,

6th computation: 256 calculations,

7th computation: 256 calculations. Considering a 256 character plain text,

8th computation: 256 calculations,

9th computation: 256 calculations,

10th computation: 256 calculations.

Thus the total computational overhead by this model is 6400 calculations.

V. COMPLEXITY OF THE MODEL

I Computation: Converting n=0:256 to Quaternary vector. Let it be QVR. The complexity is in multiples of n.

II Computation: Calculating QVR-1. The complexity is in multiples of n.

III Computation: Multiplying QVR with the key considered. The complexity is in multiples of n

IV Computation: Applying sign function on the product. Store it in QVR. The complexity is in multiples of n

V Computation: Calculating QVR+1. The complexity is in multiples of n

VI Computation: Converting output Quaternary vector to integer form. Let this be SEQ, the sequence generated. The complexity is in multiples of n

VII Computation: Converting plain text to ASCII value. The complexity is in multiples of n

VIII Computation: Adding ASCII value of plain text to sequence generated. The complexity is in multiples of n

IX Computation: Applying mod function on the output. The complexity is in multiples of n

X Computation: Converting the output to characters of the alphabet to get cipher text. The complexity is in multiples of n.

Thus, we can say that the complexity of model is **O (n).**

VI. CONCLUSION AND FUTURE WORK

We conclude here with this cloud security based algorithm using Quaternary system with a 4 digit number is used. So the sub key generated is a 4^4 i.e. a 256 digit number. By considering a Quaternary vector with a five digit number or six digit number, the length of the sub-key can be increased by 45, 46 which increase the length of sub key generated. Similarly by considering n –ary vector the length of the sub-key generated can still be increased. Thus by increasing the length of sub-key, security of cipher system can be increased still further.

References

1. Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, “Cloud security issues” In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.
2. J Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575.
3. Vikas Kumar, Swetha M.S., Muneshwara M.S, Prof S. Prakash, “Cloud Computing: Towards Case Study of Data Security Mechanism”, India International Journal of Advanced Technology & Engineering Research (IJATER)
4. Barrie Sosinsky, “Cloud Computing Bible,” Wiley India Pvt. Ltd.
5. Kaufman, Lori M. "Can public-cloud security meet its unique challenges?."Security & Privacy, IEEE 8.4 (2010): 55-57. National Institute of Science and Technology. "
6. The NIST Definition of cloud computing, Luis M. Vaquero1, Luis Rodero Merino1, Juan Caceres1, Maik Cloud Computing".p.7. Retrieved July 24 2011

AUTHOR(S) PROFILE

Arun Singh Chouhan, received the B.E in Computer Science & Engineering from University of Rajasthan, Jaipur (Rajasthan) and M.Tech from Devi Ahilya University, Indore (MP) and currently pursuing PhD in Computer Science and Engineering from Jodhpur National University, Jodhpur(Rajasthan).He is more interested in Cloud Computing, Computer Networks and Distributed system with challenges and application in computer science. He is member of various international bodies like IAENG, Hong-Kong, CSTA, New-York, USA, UACEE, USA and ISTQB, Germany.

Shalini Agarwal, received the B.Tech in Computer science and engineering from Govt. Mahlia Engineering College Ajmer affiliated to Rajasthan Technical University, Kota (Rajasthan) and currently pursing Master of Technology (M.Tech) in Computer science from Chandravati Education Charitable Trust Group Of Institute, Bharatpur affiliated to Rajasthan Technical University, Kota (Rajasthan). She is more interested in Cloud Computing and Computer networking.