INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Implementation of Reverse Caesar Cipher Algorithm for Cloud Computing

P.SUBHASRI, (M. Phil., Research Scholar) [1],
Dr. A. PADMAPRIYA, M.C.A., M.Phil., Ph.D. [2]

[1]Department of computer science & Engineering,
Alagappa University, Karaikudi- India
swarnasubha91@gmail.com

[2] Department of computer science & Engineering,
Alagappa University, Karaikudi- India
mailtopadhu@yahoo.co.in

Abstract*: Cloud computing is a large pool of easily and accessible virtualized resources, such as hardware, development platforms and services. Cloud computing is a new era of the modern world. Reasons for development of cloud computing are different people and different purpose depends upon the demand. The cloud computing flexibility is a function of the allocation of resources on authority's request. And the cloud computing provides the act of uniting. The improvement of the cloud technology also increases the security issues twice. So we need to solve the security issues in the cloud technology. The main problem associated with cloud computing is data privacy, security, data stealing, etc. In this paper we have proposed the new level of data security solution using the Reverse Caesar cipher algorithm with encryption using ASCII full 256 characters, compared between other encryption methods , our new encryption algorithm is very secured level. The main scope of this paper to solve the security issues in both cloud providers and cloud consumers using cryptography encryption methods. It is complicated to understand the cipher text compared with the other methods.*

Keywords: *Cloud computing, Security, Encryption algorithms, Caesar cipher, ASCII code.*

1. INTRODUCTION

CLOUD (Common Location independent Online Utility on Demand) is a broad solution that delivers IT as a service. Cloud computing is an umbrella term used to refer to Internet based development and services. A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery [1].

Cloud Computing [2] is a general term used to describe a new class of network based computing that takes place over the Internet. Cloud computing shared resources are provided like electricity distributed on the electricity grid.

Advantages of Cloud Computing:

a) Reduced Cost: Cloud technology is paid incrementally, saving organizations money [3].
b) Increased Storage
c) Organizations can store more data than on private Computer systems.
d) Highly Automated
e) Flexibility
f) More Mobility

2. SECURITY CHALLENGES

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft [4].

There are four types of issues [5] raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues

1. Data Issues:

Data stealing is a one of serious issue [6] in a cloud computing environment.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Data loss is a common problem in cloud computing. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire.

Solution: "*Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behavior of the cloud supplier and as a result he is confident that data is handled. Also very efficient data integrity method in cloud computing."*

2. Privacy Issues*:*

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. **Solution:** *"Authentication [7] is a best solution for the privacy issue.*

3. Infected Application:

Any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

Solution: *"To prevent [8] cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server."*

4. Security issues:

Cloud computing security must be done on two levels. One is on provider level and another is on user level. The user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action.

Solution: *"Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across.*

5. Trust Issues:

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider.

3. EXISTING METHODS

Encryption is a well known technology for protecting sensitive data. The following two papers analyze the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage.

(3.1) Parsi Kalpana, Sudha Singaraju [9] have proposed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. RSA consists of Public-Key and Private-Key. In the proposed Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

(3.2) Neha Jain and Gurpreet Kaur [10] described Data security system implemented into cloud computing using DES algorithm. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. The algorithm steps are follows.

1. Get the Plaintext.
2. Get the Password.
3. Convert the Characters into binary form.
4. Derive the Leaders (L1 to L16) from the Password.
5. Apply the Formula to get the encrypted and decrypted message.

The main contribution of this paper is the new view of data security solution with encryption, which is the important and can be used as reference for designing the complete security solution.

4. PROPOSED WORK

One of the simplest examples of a substitution cipher is the Caesar cipher [11]. It is said to have been used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages.

Further enhancement to original three places shifting of character in Caesar cipher uses modulo twenty six arithmetic [12] encryption key that is greater than twenty six.

$$En(x) = (x+n) \bmod 26$$

The most pressing weakness of this cipher is simplicity of its encryption and decryption algorithms; the system can be deciphered without knowing the encryption key. It is easily broken by reversing encryption [13] process with simple shift of alphabet ordering.

$$Dn(x) = (x-n) \bmod 26$$

The earliest ceaser cipher method include the main

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

drawbacks is plaintext and key is used only 26 alphabets.

This paper overcome the above problem to plaintext is used case sensitive, numbers and special characters in order of ASCII full characters (256 char). This proposed method providing the inverse of Caesar cipher that supports more security for the data compared with the earliest Caesar cipher. And also it can be used simply encode the message for preserving privacy. It is complicated to understand the cipher text compared with the other methods.

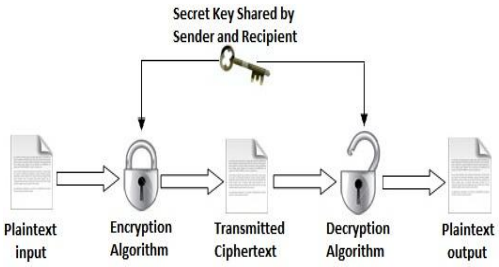

Figure 1: Encryption / Decryption Process

Encryption Algorithm

Step 1: Split the letter of the plaintext.

Step 2: Assign the position (i) of the letter.

Step 3: Generate the ASCII value of the plaintext letter.

Step 4: Assigned same Key value is considered as a key.

Step 5: To apply the below given formula:

E = (p + k + i) % 256

p – Plaintext, k – key, i – Position.

Step 6: Generate the ASCII character of the corresponding decimal value in the result from the above given formula. This would be the cipher text.

Decryption Algorithm

Step 1: Generate the ASCII value of the cipher text character.

Step 2: Here the same encryption key used.

Step 3: Assigned the position (i) of the cipher text.

Step 4: To apply the below given formula:

D = ((c – k – i) + 256) % 256

c – Cipher text, k – key, i – Position.

Step 5: Generate the ASCII character of the corresponding decimal value. This would be the original plaintext.

Example:

Encryption

Let, the character is "c". Now according to the steps we will get the following:

Step1: ASCII of "c" is 99 in decimal.

Step2: Assign a fixed key value is 10.

Step 3: Assign the position (i) is 0.

Step 4: Apply the following formula

E = (p + k + i) % 256

= (99 + 10 + 0) % 256

= 109

Step5: As per the algorithm the cipher text would be "m".

Decryption

After encrypting "c" we have got "m" as the cipher text. Now according to decryption algorithm let's try to get back the original text i.e. "c".

Step 1: 109 is the ASCII value of the cipher text character "m".

Step 2: Here, Same key "10" is used.

Step 3: Here, position (i) "0" is used.

Step 4: The formula is applied to the ASCII value 109 of the cipher text character and key 10.

D = ((c – k – i) + 256) % 256

= ((109-10-0) + 256) % 256

= 99

Step 5: "c" is the ASCII character of the decimal 99. Character "c" would be the original plaintext.

Advantages of Proposed Method

- The Algorithm is very simple in nature.
- The user can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently.
- It is case sensitive.

4.1. Results Evolution and Conclusion

Factors	***DES***	***AES***	***Blowfish***	**Reverse Caesar cipher**	
Input size	29	56	36	20	
Key size	64 bits	128 bits	128 bits	256 bits	
Cipher text	Symmetric block	Symmetric block	Symmetric encryption	Substitution cipher	

Security	Proven inadequate	Proven inadequate	Collision occurred	Security considered	
Memory	54.68	66.23	28.71	1.56	
Possible keys	56 2	128 2	128 2	256 2	
CPU usage	35	45	19	5	

Memory Utilization: Memory utilization can be calculated by using ,
Memory Utilization (%) = (Used Memory) / (Total Available Memory) * 100

From the results calculation it's analyzed that we can increase performance parameters by using proposed encryption model as compare existing methods.
Also, we can see that the AES, DES, Blowfish algorithms.
The Reverse Caesar cipher encryption techniques are better than others as they have low memory utilization time and low CPU capability.

5. CONCLUSION

Cloud computing is a new condition that is familiarizing in business surroundings where users can communicate directly with the virtualized resources and safe the cost for the consumers. Data security has become the most important issue for cloud computing security. Though many solutions have been proposed, many of them only consider 26 alphabets only. The main scope of this paper is the new level of data security solution with encryption using the ASCII full characters, which is important for designing the complete security solution.

The analysis evolutions precede the high quality of our encryption algorithm, so the level of security concludes 98%. In future we are going to implement our Reverse Caesar cipher algorithm on Google my SQL.

REFERENCES

[1] **Booth,(2004). webservice architecture. Retrived from http://www.w3.org:http//**

[2] **Cong wang, Qian wang, and Kui ren, Wenjing Lou,"Ensuring data storage security in cloud computing" at IEEE (8-1-4244-3876-1/09).**

[3] **Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.**

[4] **Cloud computing methodology, systems and applications lizhe wang, Rajiv Ranjan.http://www.unitiv.com.**

[5] **John Harauz, Lori M.Kaufman ,Bruce potter,"Data security in world of cloud computing" by IEEE computer and reliability societies,jul/Aug 2009 pp 61-64.**

[6] **Dulaney E., CompTIA Security+ Study Guide, Fourth Edition, Wiley Publishing Inc., Indiana, 2009.**

[7] **C.N. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl (2011) .**

[8] **Jagpal Singh,Krishnan lal and Dr.Anil kumar Shrotiya, Journal of Computer Science and Applications., ISSN 2231-1270 Volume 4, Number 1 (2012), pp. 1-7. http://www.irphouse.com**

[9] **Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA http://www.mytestbox.com/miscellaneous/cloud-computing-grid-computing-utility-computing-list-top-providers/**

[10] **Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security ", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.**

[11] **Security analysis of cloud computing: (http://cloudcomputing.sys-con.com/node/1330353).**

[12] **VAMSEE KRISHNA YARLAGADDA and SRIRAM RAMANUJAM "Data security in cloud computing ", vol.2 (1), pp. (15-23) (2011).**

[13] **Sara Qaisar and Kausar Fiaz Khawaja," CLOUDCOMPUTING: NETWORK/SECURITYTHREATSAND COUNTER MEASURES", ijcrb, JANUARY 2012 VOL 3, NO 9.**