Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multilevel Encryption for Ensuring Public Cloud

P.Subhasri, (M.Phil, Research Scholar)
Department of Computer science and Engineering,
Alagappa University, Karaikudi, INDIA

Dr.A.Padmapriya, M.C.A., M.Phil., Ph.D
Department of Computer science and Engineering,
Alagappa University, Karaikudi, INDIA.

Abstract— cloud computing is a new era of the modern world. The cloud computing flexibility is a function of the allocation of resources on authority's request. The improvement of the cloud technology also increases the security issues twice. The problems on the cloud computing are data privacy and data stealing. This paper has proposed Multi level of Encryption algorithms used to secure the data. Compared between other encryption methods, these methods have very secured level. This proposed method is complicated to understand the cipher text compared with the other methods.

Keywords— Cloud computing, Security, Multi level Encryption algorithms, Caesar cipher, and ASCII code.

I. INTRODUCTION

Cloud Computing [1] 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. Cloud is a broad solution that delivers IT as a service. Cloud computing is an internet based technology uses the internet & central remote servers to support data and applications. It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access.

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 [3]. 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.

II. SECURITY ISSUES

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user [5] can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are five types of issues [2] rise while discussing security of a cloud.

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

2.1 Types of cloud computing

There are four types of cloud computing models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud [8].

1. Public Cloud: The cloud computing resource is shared exterior, someone can use it and a few payments maybe count. Public organizations assist in supplying the infrastructure to carry out the public cloud [6].

2. Private Cloud: private cloud resource is boundary to a collection of people, like a staff of a company. Infrastructure of private cloud is perfectly controlled and corporate data are completely supported by the organization itself.

3. Hybrid Cloud: This is the combination of public as well as private cloud [7]. It can also be explained as multiple cloud systems that are related in a way that permits programs and data to be moved comfortably from one system to another.

4. Community Cloud: The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security).Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud [4].

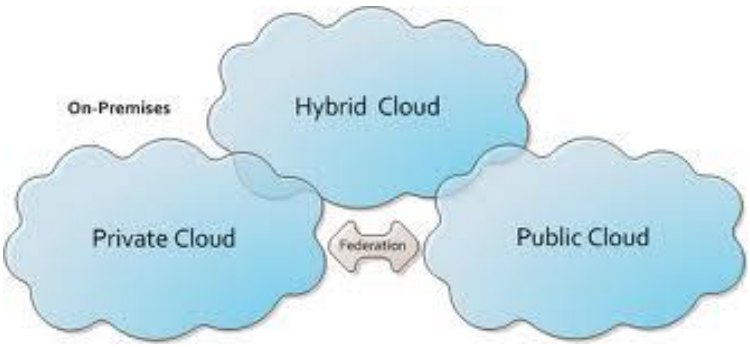


Fig. 1 Types of cloud computing

III. BACKGROUND STUDY

(3.1) Parsi Kalpana, Sudha Singaraju [10] 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 [9] 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.

IV. PROPOSED METHOD

Encryption is a well known technology for protecting sensitive data. Two types of encryption algorithms proposed in this paper.

i) Rail fence cipher algorithm for Transposition

The Rail fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows [11]. For example, using two "rails" and a message of"hellow", the ciphered writes out:

h l o
e l w

Then reads off:

h...l...o....e...l....w

ii) Caesar cipher algorithm for Substitution

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.

$$D = ((c - k - i) + 256) \% 256$$

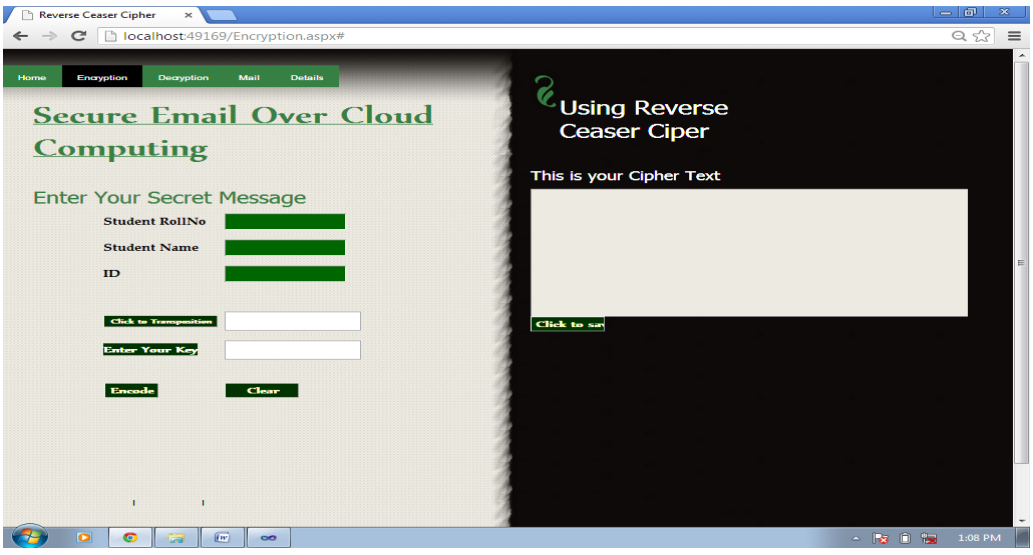
$$= ((109-10-0) + 256) \% 256$$
$$= 99$$

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

V. DEMONSTRATION OF RESULTS

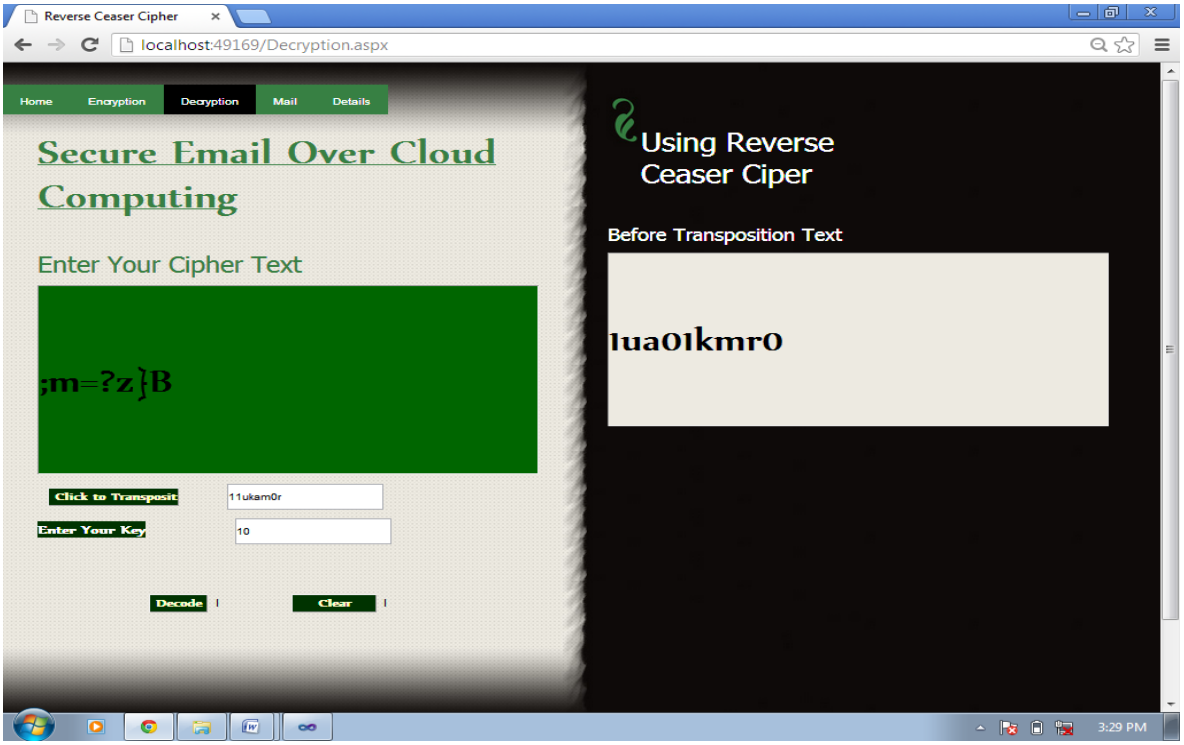
5.1 Encryption for using Transposition and Substitution Ciphers:

1. Enter student roll number, name, and id.
2. Click Transposition, the text will be encrypted.
3. Enter the key value; finally click to encode, the cipher text of the message will be displayed.



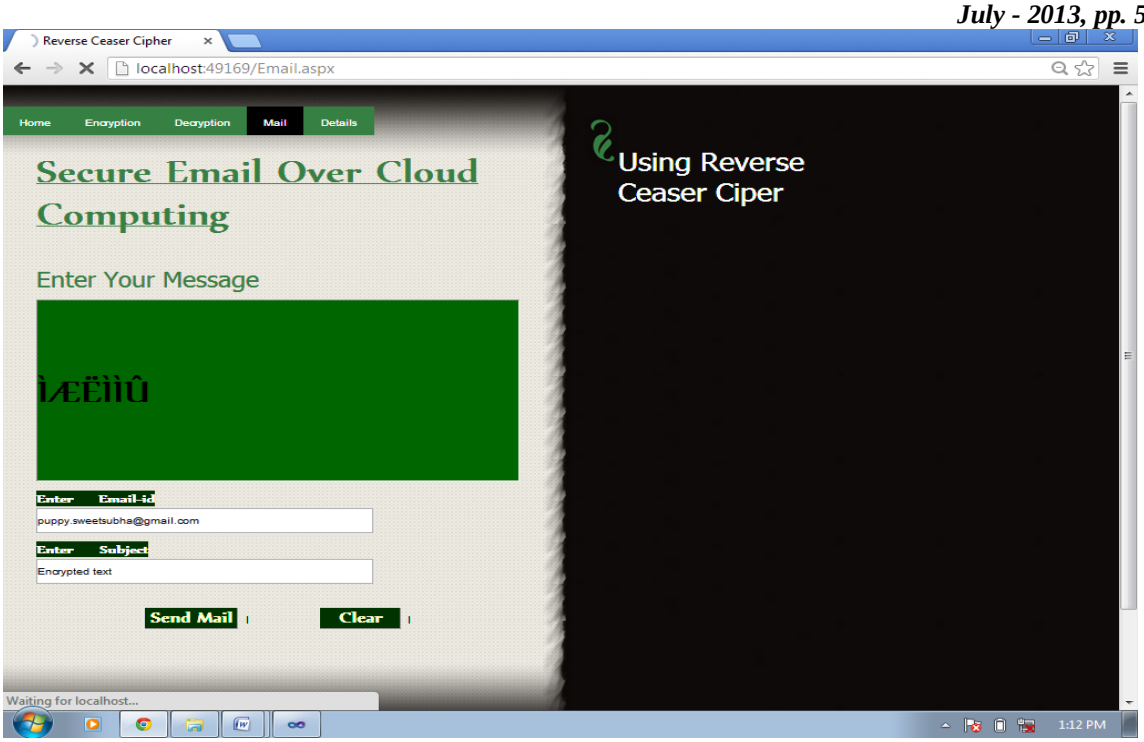
5.2 Decryption for using Transposition and Substitution:

1. Enter the cipher text.
2. Enter the key value, click the decode button, before transposition text displayed.
3. Finally click to transposition, the original message retrieved.



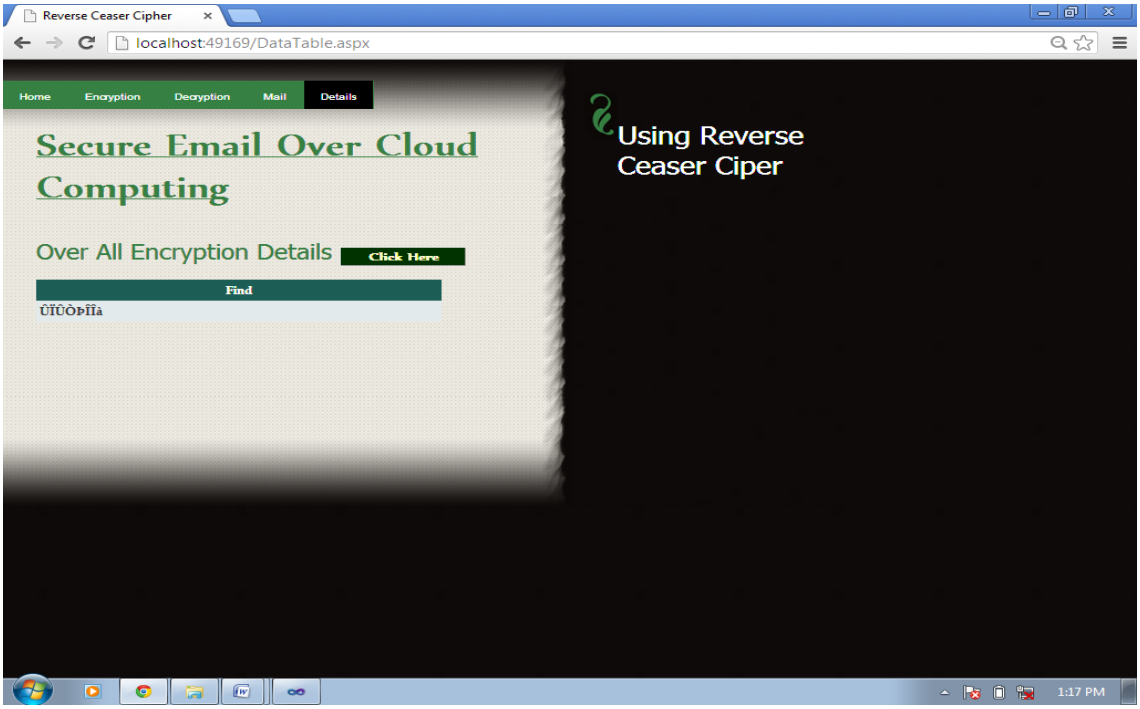
5.3 Mail Service:

1. Enter the encryption message
2. Enter mail id with subject
3. To send mail the encryption message sent to the Receiver, the receiver retrieves the message.



5.4 Database stored:

Details session include the encrypted text for preventing UN authorized users.



VI. CONCLUSIONS

Cloud computing is a large pool of easily and accessible virtualized resources, such as hardware, development platforms and services. Reasons for development of cloud computing are different people and different purpose depends upon the demand. 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. The main scope of this paper to solve the security issues in multi level encryption for both cloud providers and cloud consumers using cryptography encryption methods. It is complicated to understand the cipher text compared with the other methods. Cloud computing reduces operating cost and increases the efficiency of computing. Even though efficiency increased, still there is security threat for the data that is stored in third party area especially in Internet. Due to data security issue with cloud computing many business organization have fear in storing their data in Cloud. So the most challenging task of the business organization is to

provide high security for their data since the data are sensible related to their business. In future we have implemented this multi level encryption using the Google cloud SQL.

REFERENCES

[1] Booth.D,(2004).webservice architecture.Retrivedfrom 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] C.N. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl (2011).
[6] Dulaney E., CompTIA Security+ Study Guide, Fourth Edition, Wiley Publishing Inc., Indiana, 2009.
[7] F.A.Alvi, B.S.Choudary, N.Jaferry,"Review on cloud computing security issues & challenges", iaesjournal.com, vol (2) (2012).
[8] Gartner: Seven cloud-computing security risks InfoWorld 2008-07-02.
[9] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security ", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.
[10] 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/
[11] William, S., 2005. Cryptography and Network Security Principles and Practices. 4th Edn. PHI.

