An Implementation of Reverse Caesar cipher (RCC) Algorithm in Google Cloud using Cloud SQL

P.Subhasri (M.phil, Research Scholar) [#1], Dr.A.Padmapriya M.C.A., M.phil., Ph.D.[*2],

Department of Computer Science & Engineering,
Alagappa University – Karaikudi, India.

***Abstract*— CLOUD (Common Location independent Online Utility on Demand) is a broad solution that delivers IT as a service. Data security issue with cloud computing many business organizations have dread in storing their data in Cloud. So the most challenging task of the business organization is to provide high security for their data. The main problem associated with cloud computing is data privacy, security, data stealing, etc. To ensure the security of data, we proposed a method of providing security by implementing Reverse Caesar Cipher (RCC) algorithm using cloud SQL to the data that will be stored in the third party area.**

***Keywords*— Cloud computing, Security, cloud SQL, Google cloud, RCC algorithm.**

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.

A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery [3]. Clouds are of particular commercial interest not only with the growing tendency to outsource IT so as to reduce management overhead and to extend existing, limited IT infrastructures, but even more importantly, they reduce the entrance barrier for new service providers to offer their respective capabilities to a wide market with a minimum of entry costs and infrastructure requirements in fact, the special capabilities of cloud infrastructures allow providers to experiment with novel service types at the same time reducing the risk of wasting resources.

Cloud Computing [4] 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 Services:

Cloud computing provides different services rather than a unit of product. The basic Five types [2] of the services are as follows,

Web based cloud services: These services exploit certain web service functionality, rather than using fully developed applications.

Saas (software as a service): It is one of the ideas to providing a given application to multiple tenants, typically using the browser saas solutions are common in sales, HR and ERP.

Paas (Platform as a service): This is different types of saas. You run your own application but you do it on the cloud provider's infrastructure.

Utility cloud services: There are virtual storage and server options that organizations can access on demand, even allowing the creation of a virtual data centre.

Managed services: This is maybe the oldest iteration of cloud solutions. In this concept, a cloud provider utilizes an application rather than end users.

II. SECURITY ISSUES & SOLUTIONS

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.

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 [10] in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behaviour of the cloud supplier and as a result he is confident that data is handled."*

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. 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.

III. BASE METHODOLOGY

One of the simplest examples of a substitution cipher is the Caesar cipher [9]. 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.

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 1

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 % 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 + 256) % 256

= 99

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

IV.EXPERIMENTAL METHODOLOGY

We use the following steps to implement the Reverse Caesar cipher (RCC) algorithm in cloud.

Create Google application:

Step 1: Go to http://accounts.google.com/ and enter your Google user name, password.

Step 2: Select the own Google application link (My Applications)

Step 3: Select "create application" button, give application identifier, application title and Click Create Application "button. Now application is created.

Implement RCC algorithm in Google cloud SQL:

The following are the procedure to create Database, Tables in Google Cloud SQL and to implement RCC algorithm:

Step 1: Go to https://code.google.com/apis/console and select Google Cloud SQL option

Step 2: Select "New instance" button from the right upper corner and popup window displayed

Step 3: Type instance name and associate an authorized application, which was created earlier and click "Create instance" button

Step 4: Click instance name to see the properties associated with it

Step 5: Select "SQL Prompt" tab. All databases automatically loaded

Step 6: Create database for the application by using "create database…" query and create necessary tables

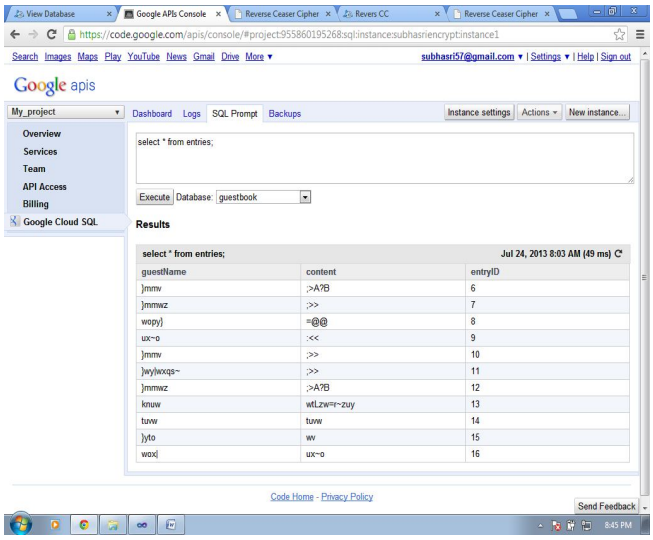
Step 7: Insert records to the tables by using "Insert into …" Query

Step 8: Create user interface for the application

Step 9: Write Java code to implement RCC algorithm in cloud and debug the application in Google cloud.

Step 10: Store the data in an encrypted format. Display the content in decrypted format while accessing.

Figure 1.Create New Instance



V.RESULTS & DISSCUSSIONS

We have created the User interface and the application by using Java and J2EE.

Step 1: Database created in Google cloud named as "Guest book".
Step 2:"Entries" table created in Guest book database and it has all necessary fields.

Step 3: An application "revcryptography" was created in Google app engine using the step given above.

Step 4: User interface designed to manipulate the Guest book details. From the home page choose link, then it displays the entry details, which is shown in Fig.2.

Step5: By clicking the "Submit Query" button the entered details received by "Submit Query" class and public key generated using RCC Encryption algorithm

Step 6: Using the public key the Entries details encrypted using RCC algorithm and stored into the table, which is shown in Fig. 1.

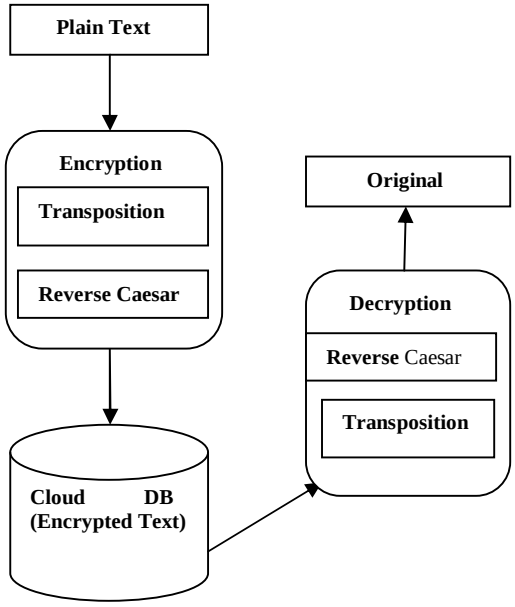
Step 7: During retrieval of data, it is decrypted after checking the generated the same key.

Step 8: Using the interface, decrypted data displayed in the form that is shown in Fig.3.

Figure 2. Google App Engine Application

Figure 3. App Engine Encrypted Database

Figure 4. Execution flow of entire process



V.CONCLUSION

The main problem associated with cloud computing is data privacy, security, data stealing, etc. 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.

In this paper, we have implemented Reverse Caesar cipher (RCC) algorithm in Google App engine using cloud SQL. From the results we obtained it is proved that RCC gives protection for the data, which is stored in Cloud. Only authorized user can retrieve the encrypted data and decrypt it. Even if anyone happens to read the data accidentally, the original meaning of the data will not be understood and it will be displayed in Encrypted text. Also we argued that the importance of security and privacy of data stored and retrieved in the cloud. We utilize RCC algorithm and Google App Engine to provide efficient and secured data storage scheme.

ACKNOWLEDGEMENT

I take this opportunity to acknowledge those who have been great support and inspiration through the research work. My sincere thanks to Prof.Dr.A.padmapriya M.C.A., M.phil., Ph.D for her diligence, guidance, encouragement and help throughout the period of research, which have enabled me to complete the research work in time. I express my deep sense of thanks to Computer Science & Engineering Department of Alagappa University, Karaikudi-India, for providing the necessary facilities during the research. And I also thank to Mr.R.Muthukumar M.C.A and colleague who have been a source of inspiration and motivation that helped to me during my dissertation period. And to all other people who directly or indirectly supported and help me to fulfil my task. Finally, I heartily appreciate my family members for their motivation, love and support in my goal.

REFERENCES

[1] Booth.D,(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] 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] William, S., 2005. Cryptography and Network Security Principles and Practices. 4th Edn. PHI.