An Implementation of RSA Algorithm in Google Cloud using Cloud SQL

N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam
School of Computing, SASTRA University, Thanjavur, Tamilnadu, India

Abstract: Aim of this study is to protect the data stored on cloud by using security algorithm. Cloud computing model advances many web applications because of its elasticity nature. This type of 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. To ensure the security of data, we proposed a method of providing security by implementing RSA algorithm using cloud SQL to the data that will be stored in the third party area.

Keywords: Cloud computing, cloud SQL, data storage security, google cloud, RSA algorithm, security

INTRODUCTION

In the modern distributed era different services offered in the Internet as a traditional hosting system. But in the traditional hosting system storage and usage are fixed. But the current trend in business requires dynamism in compute and data storage. This leads to the development of cloud model.

Cloud computing proposes new model for computing and related issues like compute, storage, software. It provides development environment, allocation and reallocation of resources when needed, storage and networking facility virtually. It satisfies the on-demand needs of the user. It facilitates the sharable resources “as-a-service” model. For the organization, the cloud offers data centers to move their data globally. It eliminates the responsibility of local nodes for maintaining their data and also cloud supports customizable resources on the web. Cloud Service Providers maintains computing resources and data automatically via software.

Data security is an important aspect of quality of service (Cong et al., 2009). As a result, security must be imposed on data by using encryption strategies to achieve secured data storage and access. Because of opaque nature of cloud, it is still having security issues. The cloud infrastructure even more reliable and powerful then personal computing, but wide range of internal, external threats for data stored on the cloud. Since the data are not stored in client area, implementing security measures cannot be applied directly. In this work, we implement RSA algorithm before storing the sensitive data in cloud. When the authorized user request the data for usage then data decrypted and provided to the user.


Whenever new features introduced then automatically reflected in the browser by refreshing it. Additional functionalities released in small sized chunks, this leads to reduce the change management hurdles. Google provides support for cloud computing and it has been updated periodically in order to meet the customers current needs after getting feedback and usage statistics from millions of customers. In order to satisfy the customer needs from anywhere the information posted by the customer is not maintained in a single site or computer, rather maintained in number of trusted nodes. Simultaneous and faster access by different users from different places is also supported by google. To get high reliability and availability the data processed by the customer is stored and updated in multiple machines. If any one node gets failed, the other one provides the service.

Google cloud SQL is very easy to use and not requiring any other software. Google cloud SQL concern, MySQL instance used and are similar to MYSQL. It is having all features and facilities provided by MYSQL. The other features are (https://developers.google.com/cloud-sql/docs/, Accessed on: January 21, 2012):

- Instance up to 10 GB
- Synchronous replication
- Import/Export databases

Corresponding Author: N. Saravanan, School of Computing, SASTRA University, Thanjavur, Tamilnadu, India
In this study, we propose a way of implementing RSA algorithm with cloud SQL to guarantee the data storage security in cloud. This approach can be either implemented by the party who stores his data or by the service provider.

**Security challenges in cloud:** Though Cloud offers sophisticated storage and access environment, it is not hundred percent reliable; the challenge exists in ensuring the authorized access. Because third parties make the decision regarding our data, security is a big concern. So cloud must ensure that the data accessed is by the trusted users. Cloud computing uses multi-domain environments and each of which having different requirements for security.

Authentication and identity management can help the users to authenticate and getting services based on their credentials (Bertino et al., 2009; Ko et al., 2009). Key issue about identity management in cloud is different kinds of protocols and its interoperability. This multi-domain issue complicates protection measures (Bruening and Treacy, 2009).

Fine-grained access control needed for cloud because of its heterogeneity of services and multi-domain access requirements. Dynamic, context based and attribute based requirements needed by the cloud. It must also ensure that the implemented policies is managed easily.

Different providers offer various services and variety of security approaches used. So a mechanism needed to ensure that dynamic interoperability among providers. But current literature has individual domain policies that are verified during integration. Thus trusted framework has to be developed to establish trust.

Whenever the organization wanted to move business data to cloud, they might have greatest fear about security of their private information. The protection against unauthorized access is the major issue for private data. So the cloud providers must give assurance to their customers regarding higher transparency for all operations and privacy assurance.

Because users may work with different places like office, home, public places and try to access the data, they should be able to use their identity in terms of digital signature and transfer data. Upcoming identity management services must be integrated with existing framework (Catteddu and Hogben, 2009). Also privacy-preserving standards have to verify the identity related attributes.

Cloud storage concern the user does not have control over data until he has been gain access. To provide control over data in the cloud data-centric security is needed. Before accessing the data it should satisfy the policy rules already defined. So cloud should enforce this scheme by using crypticraphic approaches.

**BASE METHODOLOGY**

**RSA algorithm:** We use the RSA algorithm (William, 2005) as a basis to provide data-centric security for shared data:

- Select two prime numbers.
- Calculate \( n = p \times q \).
- Calculate \( f(n) = (p-1)(q-1) \).
- Select \( e \) such that \( e \) is relatively prime to \( f(n) \) and less than \( f(n) \).
- Determine \( d \) such that \( de \) congruent modulo 1 (mod \( f(n) \)) and \( d < f(n) \).
- Public key = \{e, n\}, Private key = \{d, n\}
- Cipher text \( c = message^e \mod n \)
- Plain text \( p = ciphertext^d \mod n \)

**Experimental methodology:** We use the following steps to implement the RSA 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 our own google application link (MyApplications)
**Step 3:** Select “create application” button, give application identifier, application title and Click “Create Application “ button. Now application is ready.

**Implement RSA algorithm in google cloud SQL:** The following are the procedure to create Database, Tables in google Cloud SQL and to implement RSA 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
Fig. 1: Application ‘sampleappsaravan’ created in google app engine

Fig. 2: Hello app engine
Fig. 3: Supplier details entry

Fig. 4: Supplier details encrypted using RSA algorithm
RESULTS AND DISCUSSION

We have created the User interface and the application by using Java and JSP in Eclipse.

Step 1: Database created in google cloud named as “Sales”.
Step 2: “Supplier details” table created in sales database and it has all necessary fields about the supplier.
Step 3: An application “sampleappsaravanan” was created in google app engine using the step given above, which is shown in Fig. 1.
Step 4: User interface designed to manipulate the supplier details. From the home page choose supplier link, then it displays supplier entry form to enter the supplier details, which is shown in Fig. 2 and Fig. 3.
Step 5: By clicking the “supplier store” button the entered details received by “supplier store” class and private and public key generated using RSA algorithm
Step 6: Using the public key the supplier details encrypted using RSA algorithm and stored into the table, which is shown in Fig. 4.

Fig. 6: Execution flow of entire process

CONCLUSION

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

REFERENCES


