International Journal of Computer Science
and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 2, May 2013, 35-44

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

A PROSPECTIVE APPROACH ON SECURITY WITH RSA ALGORITHM AND CLOUD SQL IN CLOUD COMPUTING

VIJEYTA DEVI & VADLAMANI NAGALAKSHMI

Department of Computer science, GITAM University, Andra Pardesh, India

ABSTRACT

Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing, dynamic resource pools, virtualization, increases the efficiency of computing and high availability. But there are some drawbacks such as privacy, security is very important aspects. In this paper we are focusing to enhance the data security in cloud computing using RSA Algorithm and cloud SQL, 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. Google supports multi-tenant infrastructure in which, contents can be pushed in a short iteration cycle. 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. It is very easy to use and not requiring any other software. Hence authorized user can retrieve the encrypted data and decrypt data, provide efficient and the data storage security in cloud.

KEYWORDS: Cloud Computing, Cloud SQL, Data Security, Decryption, Encryption, RSA Algorithm

INTRODUCTION

Cloud Computing is the key driving force in many small, medium and large sized companies and as many cloud users seek the services of cloud computing, the major concern is the security of their data in the cloud. Securing data is always of 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 "asa-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 As a result, security must be imposed on data by using encryption strategies to achieve secured data storage and access. Because of opaqueness 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. Google supports multi-tenant infrastructure in which, contents can be pushed in a short iteration cycle., 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, My SQL 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/,):

- Instance up to 10 GB
- Synchronous replication
- Import/Export databases
- Command-line tool
- SQL Prompt
- Fully Managed
- Highly available

In this study, we propose a way of implementing RSA algorithm with cloud SQL to guaranty the data storage security in cloud. This approach can be either implemented by the party who stores his data or by the service provider Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. Every cloud service(s) seeker either an individual or a company should ask the right questions to the cloud provider before hosting their data or applications on the cloud. As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication.

DATA SECURITY ISSUES IN THE CLOUD

Data Location and Relocation

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information. Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others' resources.

Privacy and Confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety.The cloud seeker should be assured that data

hosted on the cloud will be confidential.

Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

Data Integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place For compliance purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed. When such data integrity requirements exists, that the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks).

Storage, Backup and Recovery

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

DATA SECURITY

Data confidentiality and auditability topped the list of primary obstacles for the use of cloud computing technologies in their organizations, according to a recent survey of over 1100 Indian Business Technology professionals (Figure 1).

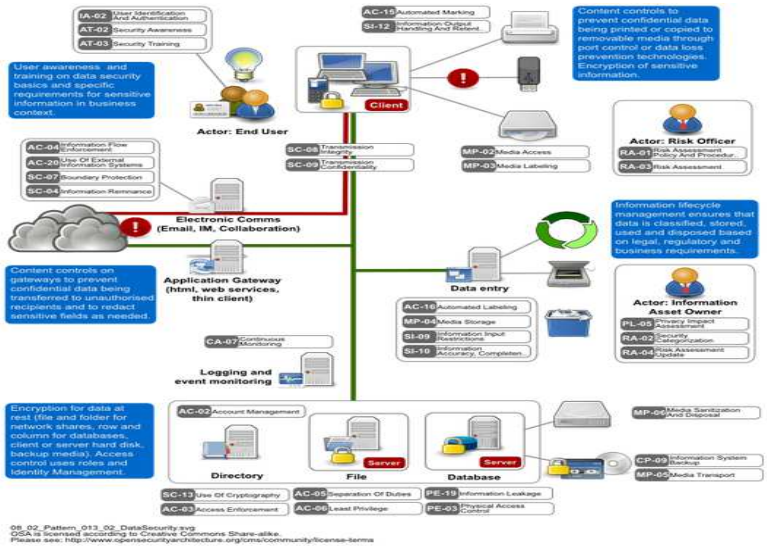

Figure 1: Data Security is Top Adoption Obstacle for Cloud in India

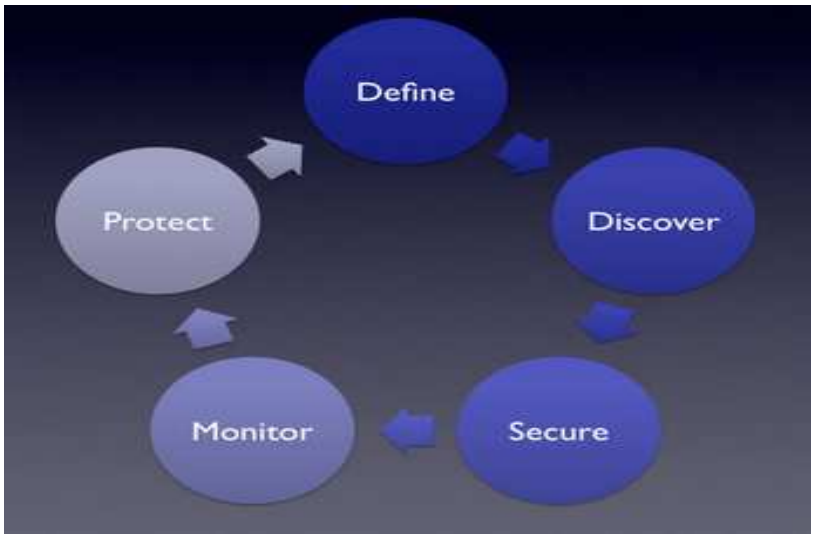

Figure 2: Data Security Cycle

The survey conducted by Saltmarch Intelligence in the third quarter of this year measured perceptions of Business technology professionals including their important challenges in adopting Cloud, the drivers, how their organization's plan to use Cloud, the different stages of adoption, and the cloud platforms, applications, clients, infrastructure and storage used. Financial savings, agility and elasticity, all enabled through cloud technology, are crucial in a fast paced business world. At the same time security incidents in the Cloud have made clear that this new promising technology comes with complexity and security and privacy challenges.

"While Data confidentiality and audit ability (24.5%) topped the list of primary obstacles for the use of cloud computing technologies, performance unpredictability (20.1%) appeared to be another key factor dampening adoption levels". Data transfer bottlenecks (17.5%) and data lock-in (14.3%) were next on the list of factors as reported by respondents. Information is produced at a rapid rate and more and more openly shared through new and agile collaboration channels that are no longer under our control.

"Hence Security of data has become a major concern. When data mobility is at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework. High levels of data relocation have negative implications for data security and data protection as well as data availability.

Thus the main concern with reference to security of data residing in the Cloud is: how to ensure security of data that is at rest. Although, consumers know the location of data and there in no data mobility, there are questions relating to its security and confidentiality of it. No doubt the Cloud Computing area has become larger because of its broad network access and flexibility. But reliability in terms of a safe and secure environment for the personal data and info of the user is still required.

PROPOSED WORK

RSA Algorithm

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public -Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA Algorithm Involves Three Steps

- Key Generation
- Encryption
- Decryption

Key Generation

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user. Steps are

- Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
- Compute n = a * b.
- Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
- Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
- Now determine d as follows: $d = e^{-1} \pmod{Ø(n)}$ i.e., d is multiplicate inverse of e mod Ø(n).
- d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
- The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
- The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps

- Cloud service provider should give or transmit the Public-Key (n, e) to the user who want to store the data with him or her.
- User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
- Data is encrypted and the resultant cipher text(data) C is $C = m^e \pmod{n}$.
- This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption

Decryption is the process of converting the cipher text (data) to the original plain text(data).

Steps

- The cloud user requests the Cloud service provider for the data.
- Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
- The Cloud user then decrypts the data by computing, $m = C^d \pmod{n}$.
- Once m is obtained, the user can get back the original data by reversing the padding scheme.

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

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 sing "createdatabase" 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 RSA 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.

EXPERIMENTAL RESULTS

In this section, we are taking some sample data end implementing RSA algorithm over it.

Key Generation

- We have chosen two distinct prime numbers a=61 and b=53.
- Compute n=a*b, thus n=61*53 = 3233.
- Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 = 3120.
- Chose any integer e, such that $1 < e < 3120$ that is coprime to 3120. Here, we chose e=17.
- Compute d , $d = e^{-1} (\text{mod } Ø(n))$, thus $d=17^{-1} (\text{mod } 3120) = 2753$.
- Thus the Public-Key is (e, n) = (17, 3233) and the Private-Key is (d, n) = (2753, 3233). This Private-Key is kept secret and it is known only to the user.

Encryption

- The Public-Key (17, 3233) is given by the Cloud service provider to the user who wish to store the data.

- Let us consider that the user mapped the data to an integer m=65.
- Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user C = 6517 (mod 3233) = 2790.
- This encrypted data i.e, cipher text is now stored by the Cloud service provider.

Decryption

- When the user requests for the data, Cloud service Provider will authenticate the user and delivers the encrypted data (If the user is valid).
- The cloud user then decrypts the data by computing, m = Cd(mod n) = 27902753 (mod 3233) = 65.
- Once the m value is obtained, user will get back the original data.

CASE TOOLS (SAMPLE DATA)

Figure 3: Application "Sampleappsaravanan" Created in Google App Engine

Figure 4: Hello App Engine

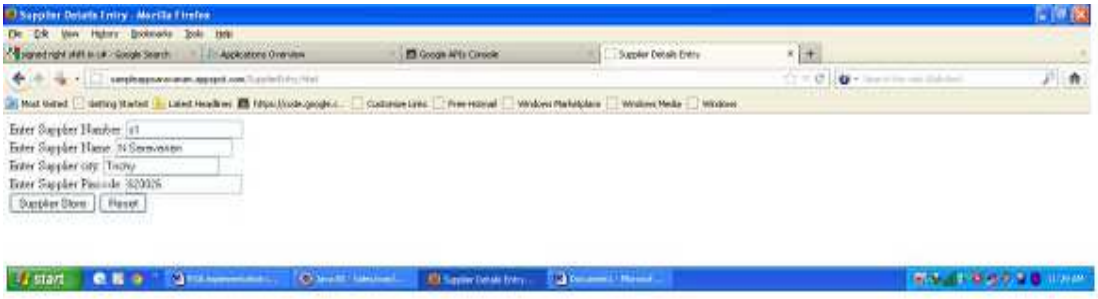

Figure 5: Supplier Details Entry

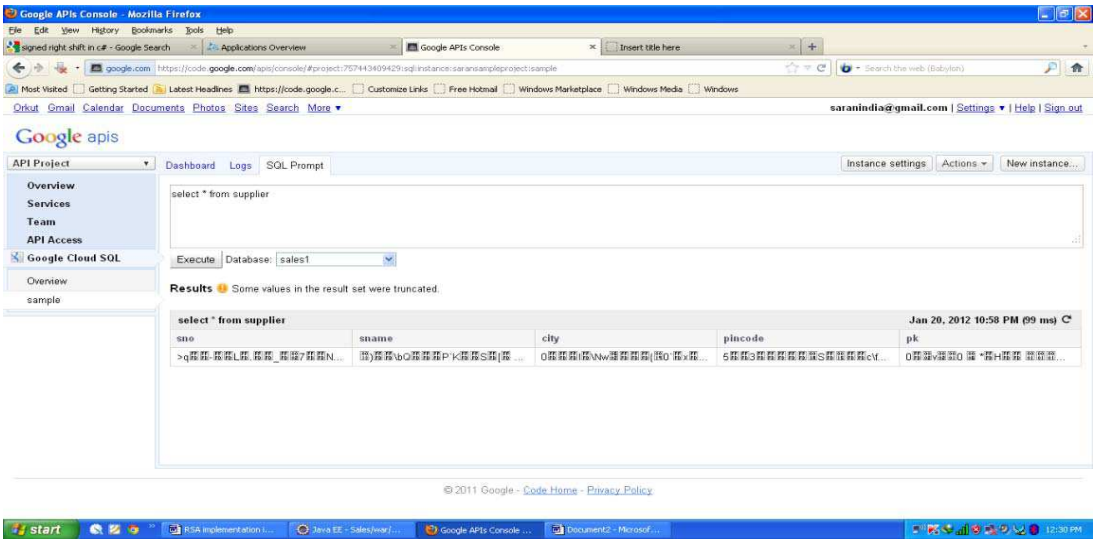

Figure 6: Supplier Details Encrypted using RSA Algorithm

Figure 7: Decrypted Data

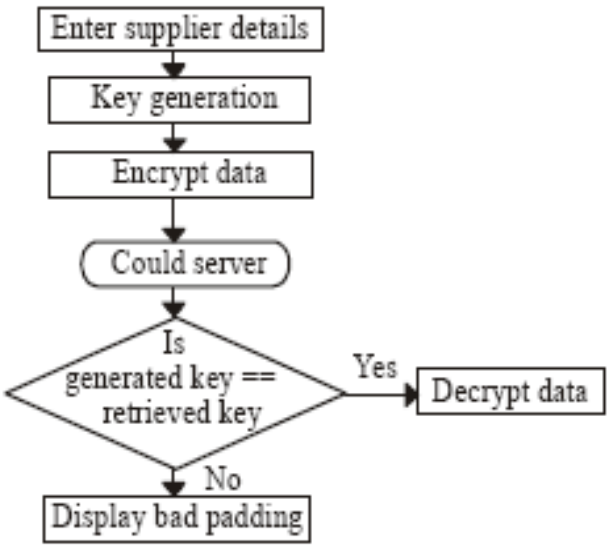

Figure 8: Execution Flow of Entire Process

CREATED THE USER INTERFACE AND THE APPLICATION BY USING JAVA AND JSP IN ECLIPSE STEPS ARE

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 "sample appsaravanan" was created in google app engine using the step given above,which is shown in Figure 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 Figure 2 and Figure 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 Figure 6.

Step 7: During retrieval of data, it is decrypted after checking the generated private key with existing private key

Step 8: Using the interface, decrypted data displayed in the form that is shown in Figure 7

CONCLUSIONS

In our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it.Hence data security is provided by implementing RSA using cloud SQL. From the results we obtained it is proved that RSA gives protection for the data, which is stored in Cloud.. 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, secured data storage, guarantee availability in the face of cloud denial-of-service attacks and the data storage security in cloud. This approach can be either implemented by the party who stores his data or by the service provider

REFERENCES

1. Amazon EC2 Crosses the Atlantic. http://aws.amazon.com/about-aws/whats-new/2008/12/10/amazon-ec2-crosses-the-atlantic/.
2. Amazon S3 Availability Event: July 20, 2008. http://status.aws.amazon.com/s3-20080720.html.
3. Amazon's terms of use. http://aws.amazon.com/agreement.
4. An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199.
5. Lithuania Weathers Cyber Attack Braces for Round 2.

   http://blog.washingtonpost.com/securityfix/2008/07/lithuani a_weathers_cyber_attac_1.html.
6. Narayanan, A. and Shmatikov, V. Robust De-anonymization of Large Sparse Datasets. In IEEE Symposium on Security and Privacy. IEEE Computer Society, 2008.
7. Salesforce.com Warns Customers of Phishing Scam. http://www.pcworld.com/businesscenter/article/139353/salesorcecom_warns_customers_of_phishing_scam.html.
8. Security Evaluation of Grid Environments. https://hpcrd.lbl.gov/HEPCybersecurity/HEP-Sec-Miller-Mar2005.ppt.
9. Security Guidance for Critical Areas of Focus in Cloud Computing.

   http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.

10. Security issues with Google Docs. http://peekay.org/2009/03/26/security-issues-with-google-docs/.

11. Shen, E., Shi, E., and Waters, B. Predicate Privacy in Encryption Systems. In TCC. 2009.

12. Shi, E. Bethencourt, J., Chan, H., Song, D., and Perrig, A. Multi-Dimensional Range Query over Encrypted Data. In IEEE Symposium on Security and Privacy. 2007.

13. Song, D., Wagner, D., and Perrig, A. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Research in .

14. Bellare, M., Brakerski, Z., Naor, M., Ristenpart, T., Segev, G., Shacham, H., and Yilek, S. Hedged public-key encryption: How to protect against bad randomness. In ASIACRYPT (2009), pp. 232–249.

15. Exploiting i-cache. In CSAW '07: Proceedings of the 2007 ACM workshop on Computer security architecture (New York, NY, USA, 2007), ACM, pp. 11–18

16. Aciiçmez, O., Koç, c. K., and Seifert, J.-P. On the power of simple branch prediction analysis. In ASIACCS '07:Proceedings of the 2nd ACM symposium on Information, computer and communications security (New York,NY,USA, 2007), ACM, pp. 312–320.