International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 5 (2014), pp. 479-484

http://www. irphouse.com /ijict.htm

# Cloud SQL Security

**Swati Srivastava[1] and Meenu[2]**

*[1]M.Tech Student, Department of CSE, Madan Mohan Malaviya Engineering College., Gorakhpur, U.P*
*[2]Department of CSE, Madan Mohan Malaviya Engineering College., Gorakhpur, U.P.*

## 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 anyone 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, security, RSA algorithm.

# 1. 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 centres 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.

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.

# 2. Data Security Issues in the Cloud

## 2.1 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 other's resources.

**2.2 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.

**2.3 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.

**2.4 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).

**2.5 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.

### 2.7 Challenges to data security

There are complex data security challenges in the cloud :

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management

### 2.8 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 (Fig. 1).

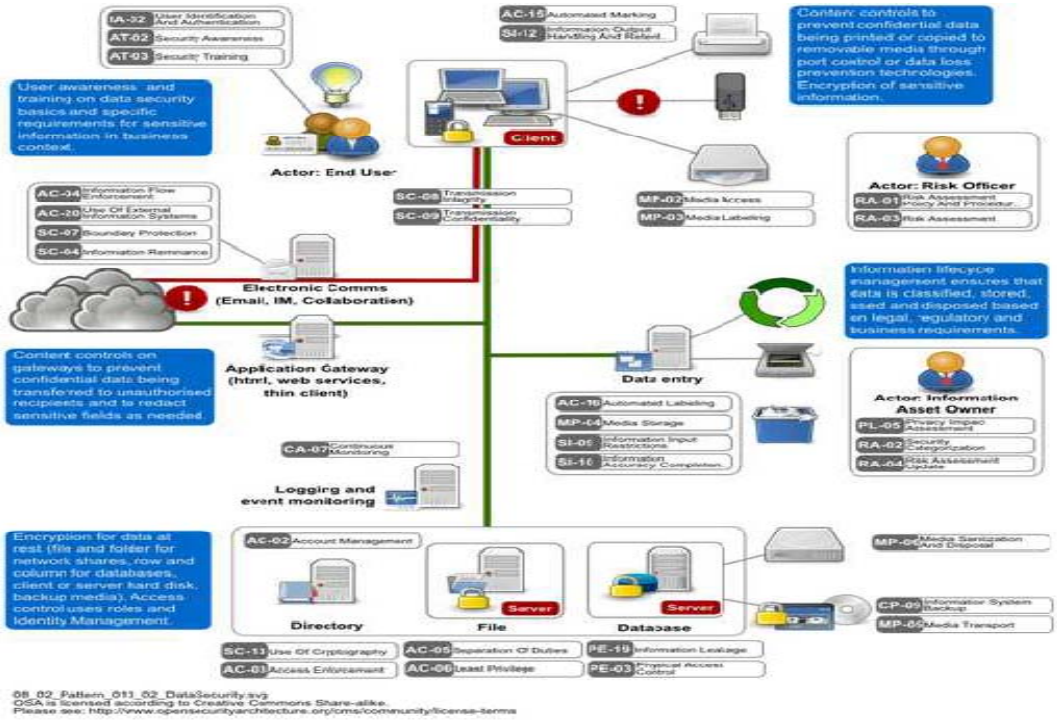


**Fig. 1**: Data Security is Top Adoption Obstacle for Cloud in India.

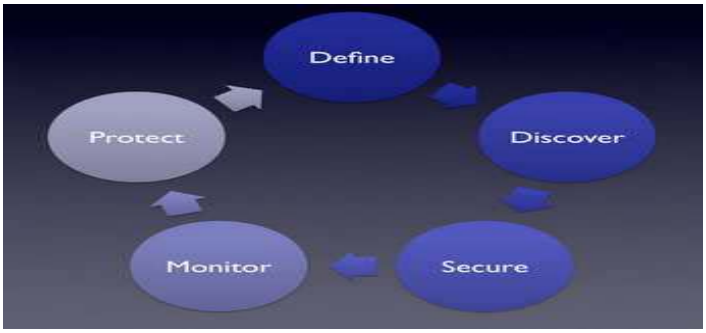


**Fig. 2**: Data Security Cycle.

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.

"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.

## 3. Proposed Work

### 3.1 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

## 4. 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-a.crosses-the-atlantic/.

[2] Amazon S3 Availability Event: July 20, 2008. http://status.aws.amazon.com/s320080720.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 Round2 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 Symposis 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.