# Cloud Computing: Data Security Using RSA

Ms. Soumya.N.S[#], Mrs. Prabha.R[*]

[#]*M.Tech Student, Computer Network Engineering,*
[*]*Associate Professor, Department of Information Technology,*
*Dr. AIT, Bangalore*

***Abstract:*** **Cloud computing is an internet based model that enable convenient, on demand and pay per use access to a pool of shared resources. It is cost effective because of the multiplexing of resources. Cloud computing is technical and social reality today, at the same time it is the emerging technology. Application data is stored in a manner that is device and location independent. Security of the cloud based applications and Data is the key concerns of the cloud computing. The principles of the security are the Confidentiality, Integrity and Availability. Cloud security is a broad topic and any combination of policies, technologies, and controls to protect data, infrastructure and services from possible attacks. This paper presents the Analysis of the Data Security using RSA Algorithm, RSA is public key based Asymmetric Cryptosystem.**

***Keywords:*** ***Cloud Security, Data security, Data life cycle, Cryptography, RSA Algorithm.***

## I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[1] The cloudcomputing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are: Cloud Software as a Service **(SaaS)**, Cloud Platform as a Service **(PaaS)** and Cloud Infrastructure as a Service **(IaaS)**. The four deployment models are: Private cloud, Community cloud, Publiccloud and Hybrid cloud.

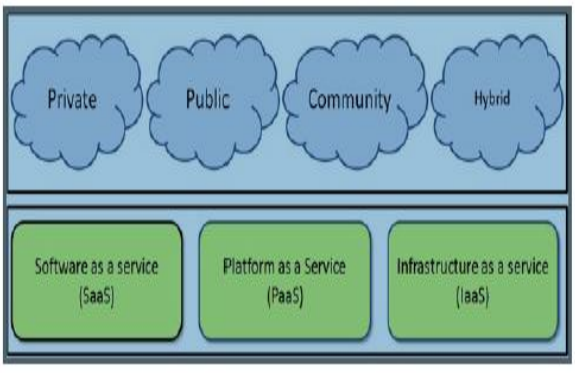


Fig.1 Cloud computing Service models and Deployment model

Cloud Computing appears as a computational paradigm as well as a distributed architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2].

### *A. Service Models*

In this section various types of service model(s) have been explained.

1) *Infrastructure as a Service Model:* service provider provides virtual and physical hardware as a service and entire infrastructure is delivered over the internet. In this model client has more security control. Provider provides networking, virtualization, servers and storage.[3]

2) *Platform as a Service Model:* provides a platform for development and deployment software applications by supporting entire application lifecycle. Cloud provider is responsible or security and monitoring. Provider provides runtime, middleware,OS, networking, servers, storage and virtualization. Developer takes several benefits from PaaS. OS features could be easily changed with PaaS. [4] Geographically distributed development tea can obtain service from diverse source and work together on software development projects.

3) *Software as a Service Model:* consumer use hosted application through a web browser. In the SaaS model, Security, management and control are services provider's responsibility because the customer has minimal control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. [5] Largely because of the relatively low degree of abstraction, IaaS offers greater tenant or customer control over security than does PaaS or SaaS.

### *B. Deployment Models*

In this section various Deployment Models are discussed:

1) *Private Cloud:* In this model cloud owner does not share their resources with any other organization. It is set up and maintained by an organization. Security can be very well implemented in this model.[6]

2) *Public cloud:* In this cloud model the resources are accessed by general public. Everybody can access easily with this cloud so it is less secure model. Cost of this cloud is not expensive. This model requires a huge investment these are owned by large organisations such as Microsoft, Google or Amazon.

3) *Community Cloud:* A cloud shares the two or more several organisations or companies for their requirements. Usually used in school or university campus.

4) *Hybrid cloud:* This type of cloud uses the one or more cloud model combinations for better use.

This paper presents a survey on the cloud data security issues, Data security life cycle. To provide security for cloud data RSA Algorithm is used, these are all discussed in the further sections.

## II. DATA SECURITY

In Cloud computing Environment there are various security issues are occurs due sharing of resources it leads to a security problem. Cloud computing as it comprises many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are pertinent to cloud computing.

Cloud possesses the security problem in Data seggregation, Data theft, unauthorised access, Uncleared Owner and responsibility of Data Protection, Data Loss conditions.[6]

### A. *Data security framework*

Security is the major concern to access the data in cloud. Security involves protecting data from being lost, destroyed or modified. [7]

1) *Protection of Data:* Data can be protected from the outside user by creating the security keys such as private key.

2) *Building Blocks:* Mathematical and cryptographic principles server as the building blocks of the security.

3) *Integrity of data:* while uploading the data the user can verify the correctness of the integrity principles.

4) *Accessing the Data:* Due to the Encryption and Decryption techniques data can be accessed securely.

5) *Authentication:* Authentication allows only authorised user to access Data in cloud.

## III. DATA SECURITY LIFE CYCLE

The life cycle of the Data security includes the six phases as shown in the following Fig. 2 once data is created it can process through all the stages.

### A. *Create*

Creation is the generation of the new digital data content, uploading and modifying the data.

### B. *Store*

Storing is the act committing the digital data storage repository, and typically occurs nearly simultaneously with creation.

### C. *Use*

Data is viewed, processed and retrieved actively.


Fig. 2The life cycle of Data security

### D. *Share*

Data is exchanged between users, customers, and partners of the respective cloud.

### E. *Archive*

Data leaves active use and enters long-term storage.

### F. *Destroy*

Data is destroyed permanently using the physically or digital name.

## IV. CRYPTOGRAPHY AND RSA ALGORITHM

The study of the Encryption and Decryption Analysis is known as the cryptography. The technique used for deciphering a message without any knowledge of the enciphering details fall into the area of Cryptanalysis.

The area of cryptography and cryptanalysis together are known as cryptology [8]. Cryptanalysis used many encryption and decryption techniques such as Caeser cipher, Monoalphabetic cipher, Play fair cipher, Hill Cipher. These techniques possess the Brute Force Attack means the attacker tries every possible key to get the original text to avoid this problem public key cryptography used.

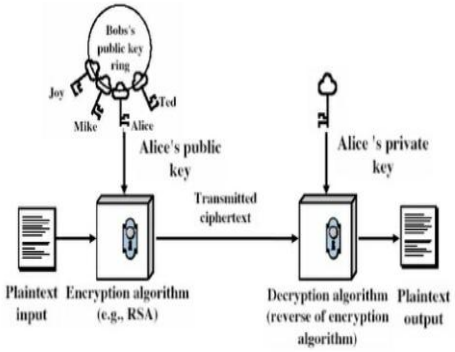


Fig.3 Public key Cryptography

*RSA Algorithmis:* the public key cryptography, in which both public and the private keys are used to secure data in

cloud. The development of the Public key cryptography is greatest and perhaps it provides a radical departure. It is also known as the Asymmetric algorithm due to the use of two key along with secret key.

***RSA*** is the deterministic encryption algorithm. It was developed by Ron Revert, Aldi shamir, and Len Adleman at MIT and first published in 1978[Rivert-Shamir-Adleman (RSA)]. In this scheme the plain text and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits.

**RSA Algorithm** involves three steps:

1) Key generation
2) Encryption
3) Decryption

*A. Key generation*

The plain text is encrypted in blocks, with each block having a binary value less than some number n i.e., for block size i bits, $2^i < n < 2^{i+1}$ .

- Input: None
- Computations:
- Select two relatively prime numbers p and q.Where n=p*q and v-(p-1)*(q-1).
- Compute the integer d such that (d*e)%v=1.
- e is the integer.

- Output: n, e and d

*B. Encryption*

- Input: Integers n, e, M
  -M is integer representation of the plain text.
- Computation: let C be the integer representation of the cipher text. $C=(M^e \bmod n)$
- Output: Encrypted text or cipher text C.

*C. Decryption*

- Input : d, n, C
- C is the cipher text.
- Computation:
- let D be the decrypted text such that $D=(C^d \text{ Mod } n)$
- Output: D is the decrypted message.
- Public Key: {e, n}
- Private Key: {d, n}

*D. Example*

- Select two prime numbers, p=17 and q=11 and M=88
- Calculate n=p*q=17*11=187
- Calculate:
  v=(p-1)*(q-1)= 16*10=160
- Select e such that e is relatively prime to v=160 and e<v that is e=7
- Determine the d such that d*e=1(mod v) & d<v. the correct value is d=23.
- Public key={7, 187}
- Private key={23,187}
- Encryption:
  $C=(88^7 \bmod 187)=11$

Decryption:

$M=(11^{23} \bmod 187)=88$

*E. Security of RSA*

Five possible approaches to attaching the RSA are [9]:

1) *Brute force Attack:* This involves trying all possible private keys.

2) *Mathematical Attack:* All the methods are used to effort the factoring the product of two numbers.

3) *Timing Attack:* It is depends on the time of the decryption of the algorithm.

4) *Hardware-Fault Attack:* This includes the Hardware-fault in the processor that generates the Digital signatures.

## V. CONCLUSION

Cloud computing provides the ondemand resources based on the computing utilities of the user request. It is the internet based model in which the Applications are used in any computer without installing it. The flexibility of the cloud is allocation of the resources ondemand. The RSA Algorithm provides the high secure and high potential Data Encryption methodology. It is highly secure than all other Encryption techniques.

## REFERENCES

[1]. Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," Version15,10-7-09, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf.
[2]. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg,
[3]. http://www.cloudsecurityalliance.org
[4]. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering.
[5]. Bhadauria, Rohit, and Sugata Sanyal. "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques." International Journal of computer applications 47 (2012).
[6]. "Data Security in Cloud Computing" T V Sathyanarayana 978-1-4673-6126-2/13/c 2013 IEEE
[7]. "Data Security Frameworks In Cloud" by Devi T School of Computing Sciences and Engineering International Conference on Science, Engineering and Management Research (*ICSEMR* 2014) 978-1-4799-7613-3/14/ ©2014 IEEE.
[8]. Subashini S and Kavitha V, "A survey on security issues in service delivery models of Cloud computing", Journal of Network and Computer Applications, Vol.34, No.1, pp. 1-11, 2011.
[9]. "Cryptography and Network Security: principle and practices" by Wiiliam Stallings sixth edition published by Pearson Education Inc@2014.