# Impact of RSA algorithm on Cloud Data Security – Analytical survey

K.Subramanian[1], M.Mohamed Sirajudeen[2]

[1]Assistant Professor, V.S.S Govt. Arts College, Pudukottai, , India
[2]J.J College of Arts and Science, Pudukottai, India

***Abstract*—***Cloud Data security and the privacy of the data access on the cloud storage in private cloud environment is a great challenge in the current era. Each and every stage of the security algorithms development mostly concentrates on the secure access for the cloud data by using different cryptographic algorithms. The research background of the cryptographic field of study focuses on the implementation of different security algorithms with higher performance in the execution. The mechanism of cloud data storage is widely using the crypto algorithms and the private cloud also give more importance for such algorithms regarding to maintain the confidential data access among the cloud service providers and clients. This research paper focuses on the Impact of RSA algorithm on Cloud Data Security – Analytical survey in both non cloud access (NCA) as well as cloud access (CA) environments on different input size of cloud data content.*

***Keywords—Cloud, Private, Security, algorithm and Performance.***

## I. INTRODUCTION

The field of "Cloud Computing" play evitable role in the current software due to the features of sharing the resources in an effective and efficient manner, efficient data storage mechanism as well as resources provided on demand whenever it will be required at suitable environment [1]. According to National Institute of Standards and Technology [2], the data to be available on the cloud will always share by the different clients under various categorization for cloud environment such as private cloud , public cloud , hybrid cloud , etc., . In general the access control is a way to confirm the authorized users for appropriate resource share/access on the cloud data [1]. According to the view of cloud data security researchers, the Cloud computing provides a high degree of data mobility, data availability, storage, backup and recovery, data integrity and privacy as well as confidentiality [3]. Cloud storage researchers are giving more focus on data security, while considering the impact of the proposed algorithms on cloud performances. Thus, modern symmetric encryption algorithms join several cloud security requirements, namely, cloud availability and compliance. In fact, these conventional schemes are typically fast and computationally less intense than asymmetric algorithms. Therefore, they are suitable for processing large streams of outsourced data [4]. In this research article concentrate on the cloud data security algorithm comparisons based on their performance analysis.

Advances in networking technology and an increase in the need for computing resources have prompted many organizations to outsource their storage and computing needs. This new economic and computing model is commonly referred to as cloud computing and includes various types of services such as: infrastructure as a service (IaaS), where a customer makes use of a service provider's computing, storage or networking infrastructure; platform as a service (PaaS), where a customer leverages the provider's resources to run custom applications; and finally software as a service (SaaS), where customers use software that is run on the providers infrastructure. Cloud infrastructures can be roughly categorized as either private or public.

## II. RELATED WORK

In a private cloud, the infrastructure is managed and owned by the customer and located on-premise (i.e., in the customers region of control). In particular, this means that access to customer data is under its control and is only granted to parties it trusts. In a public cloud the infrastructure is owned and managed by a cloud service provider and is located o -premise (i.e., in the service provider's region of control). This means that customer data is outside its control and could potentially be granted to untrusted parties [5].

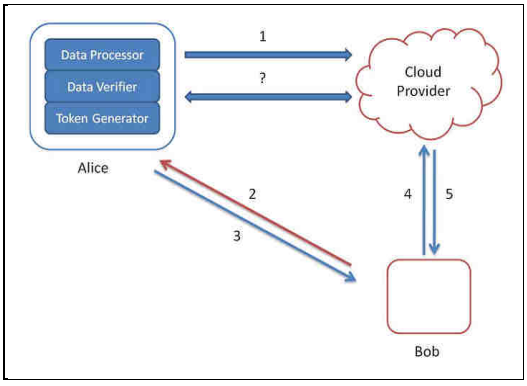


*Fig. 1: Security process on cloud*

Figure 1: (1) Alice's data processor prepares the data before sending it to the cloud; (2) Bob asks Alice for permission to search for a keyword; (3) Alice's token and credential generators send a token for the keyword and a credential back to Bob; (4) Bob sends the token to the cloud; (5) the cloud uses the token to find the appropriate encrypted documents and returns them to Bob. (?)

At any point in time, Alice's data verifier can verify the integrity of the data. Consider three parties: a user Alice that stores her data in the cloud; a user Bob with whom Alice wants to share data; and a cloud storage provider that stores Alice's data. To use the service, Alice and Bob begin by downloading a client application that consists of a data processor, a data verifier and a token generator. Upon its first execution, Alice's application generates a cryptographic key. We will refer to this key as a master key and assume it is stored locally on Alice's system and that it is kept secret from the cloud storage provider [5].

Rivest Shamir Aldeman (RSA) is the most commonly used public key encryption algorithm. RSA computation occurs with integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identity service provider.

RSA is too slow for encrypting large volumes of data. But it is widely used for key distribution Following steps are followed in RSA to generate the public and private keys [6]:

1. Conisder two large prime numbers p and q such that p~=q.
2. Compute n=p*q
3. Compute f (pq) = (p-1)*(q-1)
4. Consider the public key k1 such that gcd (f (n), k1) =1; 1<k1<f (n)
5. Select the private key k2 such that k2*k mod f (n) =1

Encryption and Decryption are done as follow Encryption: Calculate cipher text C from plaintext P such that C=P ^k1 mod n Decryption: P=C^k2 mod n=P^k1k2 mod n.

The experimental results of related work [6] mainly focus on the different category of cryptographic algorithm performance comparison based on the factor of their simulation time and buffer size. But in the proposed work experiment result discuss only the impact of RSA algorithm in Cloud based access (CA) and Non-cloud based access (NCA) environments based on the factor of performance of execution.

## III. EXPERIMENTAL RESULT

In general, the cloud data transaction under private cloud is illustrated in the following figure 2. The packet will route from source (PC0) through switch under the private cloud towards destination (PC1). While the packet come out from the source it gets encryption by using the RSA algorithm and stored in the cloud service provider (CSP) as well as it gets decrypted whenever the service is invoked by the clients .

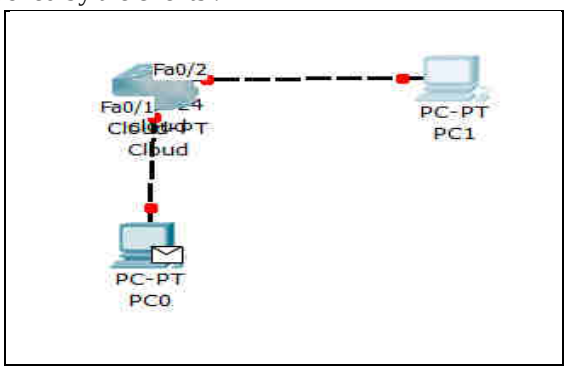


*Fig. 2: Cloud Data Transaction*

Based on the input size (Kb), the performance of execution (RSA) on Non-Cloud Access (NCA) environment takes longer time due to the reason of crypto code every time interpreted in a separate access. At the same time, in the cloud based access (CA) once it will store into the cloud service provider, it will be shared or utilized by the number clients in the onetime access of crypto code (Table 1).

*Table 1. Performance analysis of RSA (NCA&CA)*

| Input Size(Kb) | RSA (NCA) | RSA(CA) |
|---|---|---|
| 2 | 480.2 | 295.4 |
| 4 | 545.4 | 382.2 |
| 8 | 597.5 | 394.5 |
| 16 | 620.2 | 423.7 |
| 32 | 654.8 | 515.6 |
| 64 | 682.1 | 525.4 |
| 128 | 694.3 | 545.8 |

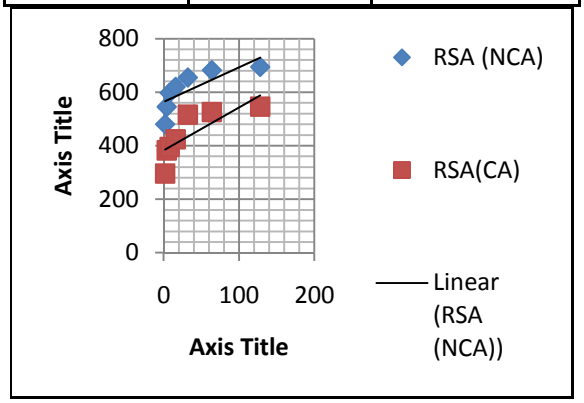


*Fig. 3: Performance analysis chart of RSA (NCA &CA)*

The performance analysis of the RSA algorithm based on the Non Cloud access (NCA) and Cloud access (CA) execution environments are evaluated in Simulation (Cisco Packet Tracer) is depicted in the figure 3.

## IV. CONCLUSION

Cloud data Security is a great challenging issue in the cloud transaction environment. Whenever, the researchers try to solve it, the cryptographic algorithm serving essential features and it provides the secure layer mechanism. In the same travelling channel, in this paper give the performance analysis of RSA algorithm and the same work try to extend it analytical survey of different algorithms as well as in future to propose a new efficient algorithm.

## REFERENCES

[1] Allen Oommen Joseph, Jaspher W. Kathrine and Rohit Vijayan, "Cloud Security Mechanisms for Data Protection: A Survey", International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.9 (2014), pp.81-90 http://dx.doi.org/10.14257/ ijmue.2014.9.9.09.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, (2011), pp. 1-3.

[3] Parsi kalpana and sudha singaraju, "Data Security in Cloud Computing using RSA algorithm", International Journal of Research in Computer and Communication Technology, page 143-146, ISSN:2278-5841, Volume-1, Issue-4, September 2012.

[4] "Cloud data storage security based on cryptographic mechanisms" by Nesrine Kaaniche - HAL Id: tel-01146029 https://tel.archives- ouvertes.fr/tel-01146029.

[5] "Cryptographic Cloud Storage", Seny Kamara Microsoft Research,senyk@microsoft.com, Kristin Lauter Microsoft Research,klauter@microsoft.com.

[6] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique ",International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, page Volume 2 Issue 4, April 2013.