# Enhanced RSA Algorithm for Data Security in Cloud

SHAMBHAVI[1], DR.SONAL SHARMA[2]
[1]*B.Tech, Department of Computer Engineering, Poornima College of Engineering*
[2]*Assistant Professor, Department of Computer Engineering, Poornima College of Engineering*

***Abstract -- Cryptography is the approach presented in the most recent decades for accomplishing Information Security. RSA is one of the generally utilized asymmetric key algorithm. The proposed work gets the data security cloud by improving the RSA algorithm. It utilizes prime numbers for encryption and decryption. The proposed calculation outflanks the standard RSA. Distributed computing is a disseminated and incorporated system of bury associated and entomb related frameworks with at least one IT assets provisioned in view of pay-on-request utilization. Despite the fact that Cloud buyers or clients are more adaptable with cloud assets, there exist different issues which cut down the use of cloud assets. Data Security issue is the real one among them. Securing the clients' information can be accomplished by the ordinary technique for Cryptography. Encryption is finished by utilizing any of the famous symmetric or asymmetric key algorithms , for example, AES, DES, RSA, Blowfish and Triple DES and so forth., RSA calculation which is a deviated key calculation utilizing two distinctive keys for encryption and decryption. The Key size can be fluctuated to influence the encryption to process solid. Consequently it is troublesome for the assailants to interfere the information.***

***Index Terms: Cloud Computing, Data Security, Confidentiality, Public Key Cryptography, RSA.***

## I. INTRODUCTION

Cloud computing is the intention control in numerous organizations the same number of cloud clients seek after the administrations of the cloud computing. The significant thing which influence the cloud computing is the security of the information in the cloud environment. Cloud computing design is a gathering of interrelated or interconnected frameworks in a conveyed way with the arrangement of sharing resources. Data Security is dependably of indispensable significance and assumes a key part in unwavering quality of figuring and because of the powerless idea of cloud and complex information in cloud security turns out to be exceptionally urgent and key. Since there is an expansion in measure of clients of cloud assets, the issues identified with getting to these assets likewise increments. There are different difficulties additionally in the cloud condition Security, Availability, Performance, Higher cost and absence of interoperability and so forth. Be that as it may, in every one of these difficulties security is the most fundamental one. On account of these reasons the use of cloud computing diminishes. Security is the real issue with respect to capacity. Data Security and Privacy, Identity and Access Management, Disaster Recovery/Business Continuity Planning and so on. A portion of the security concern, related with information called as Data Security. This issue turns into a noteworthy in the cloud computing condition, since information are dispersed in various gadgets including servers, PCs, and different cell phones. Data security in the distributed computing is more unpredictable than data security in the conventional frameworks. Secrecy assumes a noteworthy part in giving information security. Secrecy can be accomplished through the procedure of encryption and decoding which can shield the information from being access and altered by unapproved client. Cryptography has been one of the significant instrument utilized as a part of the most recent decades for dealing with the security issues. The cryptographic algorithm are of two sorts symmetric or asymmetric. Unbalanced key Cryptography otherwise called Public key Cryptography is more favored in contrast with the Symmetric key Cryptography since it isn't an issue to share the secret key to the next gathering who partake in correspondence. RSA is considered as an essential public key cryptographic algorithm for achieving the undertaking of ensuring information in the environment.

## II. RELATED WORK

RSA is a standout amongst the most achieving calculation of public key cryptography. RSA is named after its three pioneers Ron Rivest, Adi Shamir and

Len Adleman. RSA incorporates three phases: Key Generation, Encryption and Decryption. The key stage part produces two keys, to be specific, Public Key and Private Key. This Standard RSA calculation is utilized by numerous specialists to ensure the information put away in the cloud environment. Cloud Service provider gives the public key. Service provider also do the data encryption. In this manner, the information must be accessed by the approved client.

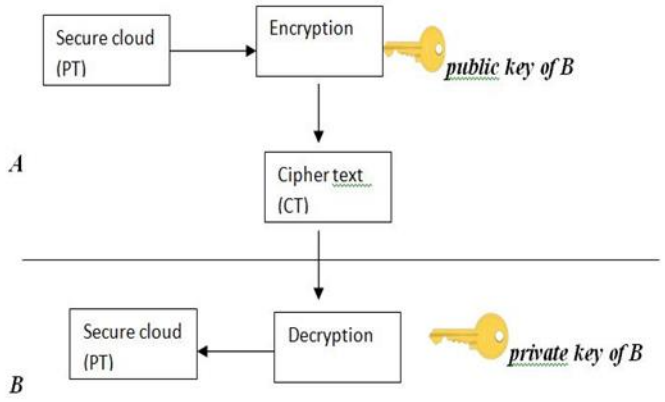
Pallav Sharma gave an answer for the security issues in the cloud environment by consolidating other symmetric key cryptographic algorithm and RSA algorithm. This approach made the procedure of encryption and decryption stronger. RSA algorithm with 1024 bit key utilized with a block cipher algorithm gave more complex encryption method. RSA and Advanced Encryption Standard (AES) calculations are utilized as a coordinated approach where information was encoded with AES and private key can be encrypted with RSA calculation. This lead to the expansion in execution and contrasted and different procedures. The parameters like throughput, reaction time, overheads and so on were utilized as an execution measure. There exist numerous variations of RSA. One among them is Multi-prime RSA. It is a separated rendition of RSA cryptosystem. . This technique was utilized to accelerate the decryption time and thus diminished the time spent for changing cipher text into plain text.

## III. PROPOSED METHODOLOGY

RSA is a Public Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first described it in 1977. RSA is an algorithm that provides security by encrypting and decrypting the data, so that only authorized user can access the data. The data is encrypted and the cipher text is then stored onto the cloud. When an user is in need of the data, the user places a request to the cloud provider, then the provider authorizes the user and provides him the data. Third-Party can detect Cloud service provider misbehavior with a certain probability by asking proof for a constant amount of blocks that are independent of the total number of file blocks [4]. Every message block is mapped to an integer value. RSA algorithm consists of Public Key and Private Key. Public Key is known to all cloud users, whereas Private-Key is known only to the user who originally owns the data. Encryption is performed by the Cloud service provider and decryption is performed by the Cloud user/cloud customer. Once the data is encrypted with the Public Key, it can be decrypted with the corresponding Private Key. Figure 2 outlines the working of RSA algorithm.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption




RSA algorithm involves two keys termed as public and private. The public key is used for encryption process and private key is used for decryption. Both the keys use the same computed 'N' value. The proposed Enhanced RSA (ERSA) algorithm uses two different 'N' values for encryption and decryption

The three Stages of the ERSA algorithm:

Stage 1: Key Generation

Stage 2: Encryption

Stage 3: Decryption

Stage 1: Key Generation involves the following steps.

STEP 1: Select any two large prime numbers P and Q. Apart from these, choose two more prime numbers PR1 and PR2.

STEP 2: Calculate the values of N1 and N2 by

N1 = P * Q * PR1 * PR2

N2 = P * Q

STEP 3: Compute Φ(r) = (P-1) * (Q-1) * (PR1-1) * (PR2-1)

STEP 4: Choose the Public Key E, such that GCD (E, Φ(r)) = 1.

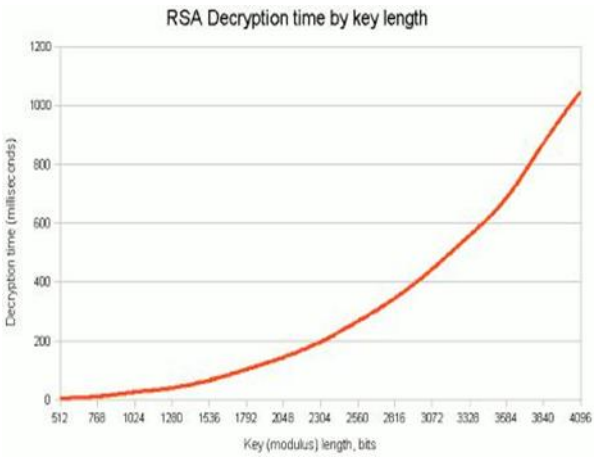
STEP 5: The Private Key D is computed from D * E = 1 * mod (Φ(r)).

Thus, the Public key component has a pair of E and N1 and Private Key pair as D and N2.

Stage 2 : Encryption Process The formula for generating a cipher text from the given plain text is C = ME mod (N1).

Stage 3 : Decryption Process The Plain text can be found by using M = CD mod (N2).

The proposed algorithm ERSA used RSA algorithm with computations of two 'N' values. The calculated N1 and N2 values included prime numbers instead of two Random Numbers as in High Speed and Secure RSA algorithm. The ERSA algorithm increases the encryption speed and decreases the decryption time.




## IV. PERFORMANCE ANALYSIS

The Multi-specialist quality based encryption algorithm gives intrigue protection against any number of conspiring clients. Every expert's characteristic set must be disjoint. To beat this issue, a different duplicate of each property for every condition might be made. The CA can decrypt each cipher text so the client security and privacy of the information is less in this framework.

The framework structure of RSA algorithm depends on the number hypothesis. It is the most security framework in the key frameworks. An outsider can't break the private key in light of factorization of bigger numbers. In the event that you need to break the data, you have to deteriorate a substantial number. So as to make the RSA wellbeing, it must pick an extensive incentive for x and y. Clients' normally decision in excess of 100 decimal digits, with the goal that the aggressor can't decay the N in polynomial time powerful inward. The RSA encryption and decoding calculation require a considerable measure of figuring and the speed is moderate when contrasted and the symmetric cryptographic algorithm. Size of the key is conversely corresponding to security. With a specific end goal to expand the level of security the extent of the key ought to be more prominent. On the off chance that the size is long the computational speed will be more prominent.

## V. CONCLUSIONS AND FUTURE WORK

Cloud computing is as yet another and advancing worldview that if registering is viewed as on demand service. Once the association takes the choice to move to the cloud it loses control over the information .Thus measure of insurance expected to secure information is straightforwardly relative to the estimation of information. Security of cloud depends on confided in registering and cryptography. The above given investigation demonstrates that utilizing prime numbers in public key cryptography calculations upgrades the security. Adding to its security, making the procedure of transformation of plain content to figure content and the other way around is more perplexing a result of the consideration of two more prime numbers. The proposed calculation ERSA has been actualized such that it makes a complex computation, as well as expands the speed of encryption and decryption time to a specific degree with the assistance of two diverse 'N' values. It is watched that there is a little variety in decryption time when the record estimate is expanded. In future, the Chinese Remainder Theorem can be connected in decryption process.

REFERENCES

[1] D.I.George Amalarethinam and H.M.Leena "Enhanced RSA algorithm for data Security in cloud".

[2] Karthija.T,Dr.A.S.Radhamani,V.G.Anisha Gnana Vincy,L.Amutha Swaminathan "an overview of security algoriths in Cloud computing."

[3] https://www.nist.gov/sites/default/files/ documents/itl/cloud/cloud-def-v15.pdf

[4] Nasrin Khanezaei, Zurina Mohd Hanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", IEEE, 58-62, 2014.

[5] Sarthak R Patel, Khushbu Shah, "Security Enhancement and Speed Monitoring of RSA Algorithm", "International Journal of Engineering Development and Research", 2, 2057-2063, 201