



SECURED ALGORITHM FOR CLOUD STORAGE SECURITY

B. Ramya Sri¹, Dr.R.CH.A.Naidu²,
K.Meghana³, B.Pavani⁴

^{1,3} Department of IT,SMEC,
Hyderabad -500014

² Department of CSE,SMEC,
Hyderabad -500014

⁴ Department of IT, MLR Institute of Technology,
Dundigal,Hyderabad-500043

June 12, 2018

Abstract

Cloud gives clients an efficient, scalable, economical approach to share and save data in with low maintenance and infrastructure cost to maintain data. In view of repetitive change of membership and repeated requirement to use information, security or confidentiality of information altered into the testing issue. For the existing schemes, distributing key on safer communication channel is impossible in reality. Hence a more secure algorithm is in need. This paper portrays RSA estimation in which data to be set in cloud is enciphered before sparing it in cloud. RSA algorithm needs two keys namely public key, private key where encryption is completed by utilizing open key, then deciphering is done by private key.

Keywords:Security, encryption, Cloud Storage, decryption, RSA algorithm.

1 INTRODUCTION

Cloud Storage used to store objects used for developers and enterprises. Distributed storage in cloud straightforward and versatile approach to hold, access, and trade information through the network. Cloud storage usage excludes the accomplishment and management costs of buying and maintaining own storage infrastructure for the enterprises or individual developers. It increases the ways to utilize the information "anywhere, anytime", provides global scale.

The upsides of this concept usage in enterprises let them to compensate only for the space they use. Cloud storage act as a usual failure evidence for the endorsement of information as 2 to 3 backup servers are maintained and these backup servers are located and maintained in distinct locations throughout the world. It acts like internal storage for our system by using the protocol named as WebDAV. For organizations, it acts as an essential and important file server. Cloud data storage allows transmission of following areas:

1. The price of Ownership: With cloud storage, hardware purchase is not needed or no capital will be invested. One can augment or reduce the size of infrastructure on demand, can change performance and retention characteristics, and required to spend money for storage space that was actually used. Data which was accessed less frequently can be passed automatically to the tiers with less cost to decrease the charge of keeping up the framework or infrastructure.
2. Time to Deployment: Cloud storage lets IT to deliver the space as and when needed. Hence developers can work to resolve complex problems instead of than managing storage systems.
3. Information Management: By Cloud storage, information can be survived by tiering automatically or locking the data to validate compliance of requirements.

As the usage of distributed storage is mounting quickly day by day at enterprise level, there must be a provision to employ a secure way to use data. Storing information in Cloud is efficient and simple

to use which gives employees the access to their data anywhere, at any time, on nearly any device, giving security to cloud is a best issue for associations' IT and security offices.

Because of the favours obtained by the Cloud storage, this is adapted by multiple enterprises and security in distributed storage in cloud becomes the major matter of interest is to keep the data secure and safe. Enterprises should use additional security methods to provide more safety to information in support of the basic protection mechanisms given by providers. The development of IoT technology lets enterprises more dependent on cloud technology.

2 RELATED WORK

The major challenges with cloud security is that the employees of the organization use free file exchange and cloud services that are not proposed by the organization which may not gratify the security principles established.

In addition to implement the security solutions, to avoid unauthorized use to the delicate information, it is imperative that organizations must train their employees about the risks imposed by exchanging and saving information in cloud. Organizations must consider the measures to relieve from these risks. To provide Cloud Storage Security, cryptographic techniques are used.

Encryption is the proposal of encoding the information existing in cloud to create a scrambled form of it. The methodology of encoding is encryption, Decoding is unscrambling. The keys for encryption, decoding of data are open key, private key which are essential to apply the methods of cryptography. For the most, 2 classes of cryptographic policies are utilized: symmetric and asymmetric or unbalanced. Symmetric Techniques consider single key for the procedures of encryption, decoding while unbalanced systems include the utilization of open key, private key. This article presents a short depiction of the cryptographic method, RSA calculation is provided to offer security to the information. The accompanying areas will give an outline of how RSA calculation functions.

3 RSA ALGORITHM

RSA (Rivest Shamir Adleman) calculation was proposed in 1978. It is an unbalanced cryptographic strategy which is in necessity for current PCs i.e. it utilizes 2 keys where open key is freely known, private key is mystery.

The progression of RSA is as the following: RSA produces open key utilizing 2 prime numbers. The prime numbers used to deliver open key are kept secret as these are utilized to create private key. If one can factorize general society key, and after that the mystery of private key is traded off. In this manner encryption quality absolutely relies on the key size.

RSA calculation is executed in four stages:

1. Key generation
2. Key circulation
3. Encryption
4. Decryption

3.1 Key Generation

Using RSA calculation, keys are created as underneath:

1. Choose any two prime values p and q discretionarily, comparable in greatness and vary long.
2. Ascertain n as $n = pq$ where n goes about as modulus for open key and secret key. Length of n is taken as key length.
3. Compute $\lambda(n) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p-1, q-1)$, where λ is Carmichael's totient function. $\lambda(n)$ is kept secret.
4. A whole number e is picked to such an extent that $1 < e < \lambda(n)$ and $\text{gcd}(e, \lambda(n)) = 1$; i.e., e and $\lambda(n)$ are coprime. Find value of d as $d = e^{-1} \pmod{\lambda(n)}$; i.e., d is modular multiplicative inverse of e . Finally, e acts like a public exponent and d as private exponent. Public key is combination of n and e . Private key is mix of n and d which are mystery. p , q , and $\lambda(n)$ are likewise kept as they are utilized to create the estimation of d .

3.2 Key circulation

Assume that A needs to associate with B where they are utilizing RSA to information exchange, A ought to have B's open key for the method of encryption and B utilizes the secret key to decipher the information. To permit A to send information, B transmits his open key (n, e) to A through a dependable course however he ought to never share his secret key i.e. d .

3.3 Encryption

After knowing B's open key, A can send information D to B. To send information, D have to be changed to number m , $0 < m < n$ by utilizing Padding plan. Then cipher text c will be generated using B's public key as

$$C = m^e \pmod{n}$$

This cipher text is transmitted to A.

3.4 Decryption

Now B can get information D from c utilizing his secret key type d by

$$C^d = (m^e)^d = m \pmod{n}$$

3.5 Challenges with RSA

If little encryption examples are used for encryption, little estimation of m , at that point resultant figure content will be decoded effortlessly.

Attacker can initiate a plain text attack towards the cryptosystem. Attackers make a dictionary by encrypting likely plain texts using public key, stores resulting cipher texts. At that point by watching the communication channel, if any match occurs with cipher texts available in dictionary, attackers use this dictionary to know about the data sent. To move around these challenges, RSA must be used with padding schemes. Padding schemes guarantee that M does not get into scope of unreliable plain messages. Once a certain text is padded, it will be encrypted to scramble to different cipher texts available which degrade the attackers capability by increasing cost of maintaining

a dictionary. The above steps describe RSA algorithm briefly. If the data is to be placed in cloud, it must be encoded before. One who is in need of the information from cloud can get it by private key of enterprise or organization.

This is one member of cryptographic policies to employ security in distributed storage in cloud by saving the encrypted data in cloud.

4 CONCLUSION

In this article, RSA algorithm was explained with different phases of it. By this method, security in distributed storage in cloud is gained by encoding the given information before saving it. This is not the only algorithm for cloud storage security. This paper can be enhanced in future by considering different strategies for scrambling the information, for example, Elliptic Curve Cryptography with better key quality, altered RSA calculation and so on.

References

- [1] N.B.Mahesh Kumar, "Encrypted Bigdata Using AES Deduplication in Cloud Storage", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 7 July 2017, Page No. 21889-21894
- [2] Douceur, et al., Reclaiming space from duplicate files in a server less distributed file system in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2002, pp. 617624.
- [3] Wallace, et al., Characteristics of backup workloads in production systems,inProc.USENIX Conf. FileStorage Technol., 012, pp.116.
- [4] Wei, et al., Security and privacy for storage and computation in cloud computing, Inf. Sci., vol. 258, pp. 371386, 2014.
- [5] Xin Zhou, Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption".

- [6] Nentawe Y. Goshwe, “Data Encryption and Decryption Using RSA Algorithm in a Network Environment”, IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 9.
- [7] Lu Chang, Xu GuangMing, “Research and Implementation of File Encryption and Decryption”, Advances in Computer Science and Engineering pp 165-170.
- [8] Farheen Sultana , Bikiran Choudhury , Shobha M.S ,Dr.Jitendranath Mungara,“A Study on Data Encryption Using AES and RSA”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2017.

