ISSN 2395-1621

A Survey: Data Security in Cloud Computing Based on RSA

[#1]Prof. Pournima More, [#2]Kajal Temgire, [#3]Pratiksha Kamble, [#4]Dhanshri Chavan, [#5]Laxmi Dehade

[1]pournima.more1@gmail.com
[2]luckydehade95@gmail.com
[3]dhansharichavan1@gmail.com
[4]kajaltemgire@gmail.com
[5]ritukamble@gmail com

[#12345]Department of Computer Engineering

G.H.Raisoni College Of Engineering, Wagholi, Pune.

ABSTRACT

In this system an effective solution to enhance the security of data. Information security has become an important issue in data communication. We are using cryptography and Stegnography concept for providing security. In cryptography encoding message to make them non readable from to secure data over the network. In other hand of Stegnography we hiding existence of data. The objective of this proposed method is to provide more security to user data. To provide cryptography we are using our modified RSA algorithm and to provide Stegnography we are using Texture pattern to embed data. In this system new approach we used modified public key cryptography and Stegnography texture pattern to increase size of embedding message. We providing security to data when we are uploading data on cloud computing.

ARTICLE INFO

Article History

Received: 31st October 2016

Received in revised form :

31st October 2016

Accepted: 3rd November 2016

Published online :

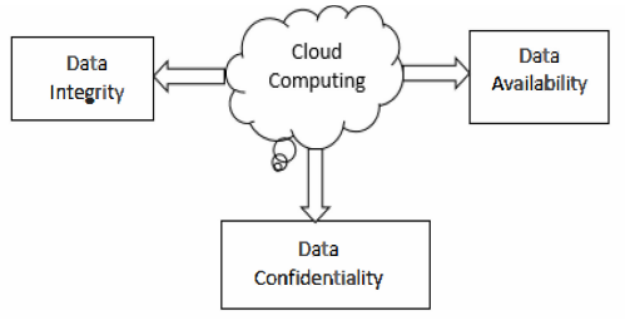
10th November 2016

Keywords: RSA ,Steganography, Secure hash algorithm , Public key cryptography

I. INTRODUCTION

Cloud computing is the idea of moving the localized computer programs, data and processing to an Internet server for easier and more secure access. Cloud computing consider as a next generation technology that revolutionized the IT industry. Cloud computing provides huge infrastructure to perform tasks and store data. The cloud customer does not want to work with single cloud provider due to compatibility issue, service availability issue and sometime insider problem. So they are use multiple cloud services according their need. User of cloud transfer their applications and data to the cloud environment, so it is necessary that the security method provided in the cloud are better than traditional methods. Unauthorized access of data, network and application by an unauthorized person (hacker) are cause lack of security and protection for cloud environment, which effects productivity and growth of the organization . To determine the level of risk durability and concentrate on reducing the risks is the one of the most important part of cloud that cannot be neglected by the cloud service provider. Cloud computing have some important feature that overcome the feature of traditional services and prove the importance in growth of IT industry.

Cloud computing is based on network and computer applications. In cloud data sharing is an important activity. Small, medium, and big organization are use cloud to store their data in minimum rental cost. In present cloud proof their importance in term of resource and network sharing, application sharing and data storage utility. Hence, most of customers want to use cloud facilities and services. So the security is most essential part of customer's point of view as well as vendors. There are several issues that need to be attention with respect to service of data, security or privacy of data and management of data. . Rivest, Shamir and Adlemen (RSA) algorithm was most widely used to provide security technique. Here we have modified the RSA algorithm to enhance its level of security. This paper presents Modified RSA algorithm along with time and security by running several encryption and decryption.



Data Integrity : Data integrity assure that the information is absolute and valid. Integrity include controlling the network device and data from the unauthorized access or maintain them strictly. Cloud service provider should ensure about data integrity and provide trust to the user for their data privacy or security.

Data Availability: Availability define as all the data and information are continually available at a required level that are requested by customer. So we can say that all machines have to stored data and application and deliver or process information when the user need them.

Data Confidentiality: Basically data confidentiality refers to a set of rules that limits access of information or data and keep confidential from outsider.

The positive large number is easily factorized or break and less prime number are easily decomposed which will not provided more security over the network, that's why we used two key, co-prime number and bit shifting to provide more security over the network .

In this research paper we developed an algorithm it is based on modified RSA algorithm based on public and private key, co-prime number and bit shifting. This algorithm provides high security over the network and secure data transfer on the cloud using steganography texture pattern. In steganography texture pattern the data is embedding in multiple pixel

II. RELATED WORK

Cryptography is a process which is associated with encloses plaintext into cipher text (encryption process) then back again plaintext (decryption).In Asymmetric key cryptography using two different keys: public key and private key .private key cannot obtain by public key. This is one major difference between asymmetric and symmetric key cryptography, and that major difference change whole process. mostly it has implication throughout the security.

We use the new methodology of encryption and steganography on cloud server. Here we use the local server for performing the modified RSA algorithm and steganography techniques perform proposed system.

Proposed RSA algorithm

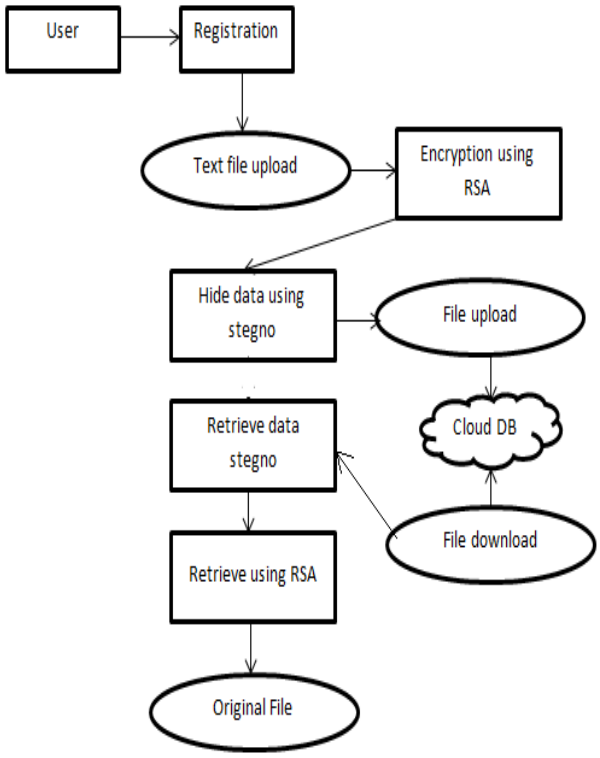


Fig 1. System architecture

III .METHODOLOGY

SHA

The SHA i.e. Secure Hash Algorithm is basically based on the concept of hash function. The basic idea of a hash function is that it takes a variable length message as input and produces a fixed length message as output which can also be called as hash or message-digest. The trick behind building a good, secured cryptographic hash function is to devise a good compression function in which each input bit affects as many output bits as possible. It is used with the Digital Signature Standard (DSA) for digital signature so it has a particular importance.

RSA

RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. In this paper, we have develop a new algorithm for generating signature that overcomes the shortcomings of the RSA system. In addition, the new algorithm achieves high security for data.On the receiver part, the message is verified by using sender's public key and his private key to decrypt the message successfully. Also we compare the Hash value of Modified RSA and Steganography Hash Value.

Algorithm Steps:

Step 1:
Implement RSA() algorithm
bitlength = 1024

Step 2:
Generate random number:
r = new Random();

step 3:
Calculate integer number with bit length
p = BigInteger.probablePrime(bitlength, r);

step 4:
Calculate second number with bitlength
q = BigInteger.probablePrime(bitlength, r);

Step 5:
Multiply both number p * q
N = p.multiply(q);

Step 6:
Calculate GCD

Step 7:
Calculate mod inverse value

Step 8:
Encrypted message by RSA

STEGANOGRAPHY:

Steganography used for hide the private data on image, after you can use for authenticate that image. provides high security over the network and secure data transfer on the cloud using steganography texture pattern. In steganography texture pattern the data is embedding in multiple pixel.

IV.APPLICATION

Steganography Using Texture Synthesis method is used widely for many real world application

Some of the application areas are:
1. Online Shopping
2. Banking

V. CONCLUSION AND FUTURE SCOPE

We conclude that in this paper is, RSA implements a public-key cryptosystem that allows secure communications. We combine Modified algorithm and Steganography for security. In this paper efficient implementation of RSA algorithm is used to encrypt and decrypt the data.

This proposed work would be inspiring for advance research such as secure transmission of file, video file, image file, etc. this may perhaps our future research topic using hybrid data encryption and decryption approach.

REFERENCES

[1] RSA.com. (2011). RSA history. Retrieved Decembers8,2011from<http://www.rsa.com/node.aspx?id=2760.>.

[2] ChaitaliBobade, IramnaazPathan (2015) They uses concept includes the texture synthesis process into steganography to hide secret messages IOSR Journal of Electronics and Communication Engineering (IOSR-JECE).

[3] Alok Kumar Shukla,V.KapoorIJESRT (2015) They discus problem positive large number is easily factorized or break and less prime number are easily decomposed which will not provide more security over the network.

[4] Saranya Vinothini, VasumathiIJCSIT 2014 They also find the security problem on data transferring.

[5] Robinson, S. (2003). Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. SIAM News, p. 6.

[6] Tariq Alturkestani&Saeed Al Jaberi, RSA-Algorithm for PublicKey Cryptography.

[7] Boneh, Dan (1999). "Twenty Years of attacks on the RSA Cryptosystem". Notices of the American Mathematical Society 46 (2): 203–213.

[8] Håstad, Johan (1986). "On using RSA with Low Exponent in a Public Key Network". Advances in Cryptology — CRYPTO ’85 Proceedings. Lecture Notes in Computer Science 218. pp. 403–408.

[9] Coppersmith, Don (1997). "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities". Journal of Cryptology 10 (4): 233–260.

[10] Bidzos, Jim, "Threats to Privacy and Public Keys for Protection", COMPCON Spring '91 Digest of Papers, IEEE Computer Society Press, p. 189-94.

[11]Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publication Company Limited page no. 32 2003.

