ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm

V.Masthanamma[1],G.Lakshmi Preya[2]

UG Scholar, Department of Information Technology, Saveetha School of Engineering

Saveetha University, Chennai, Tamil Nadu, India[1,2]

ABSTRACT: Nowadays cloud computing is emerging technology which gives open resources on the internet. It is offering large amount of data to the users and distributed data over the network. But the main issue is it does not have any security in distributing data. It becomes the main obstacle in cloud computing environment. So to enhance the security, we proposed an algorithm called RSA algorithm. It is a new approach and it met the requirements of public-key systems. By using this algorithm it will increase the security in data and consumes less time and less cost.

KEYWORDS:cloud computing, distributed data, security, RSA algorithm

I. INTRODUCTION

Cloud computing denotes sharing of resources rather than having local servers to handle applications. It provides services to servers, storage and applications over the internet. And this cloud computing environment is used by all small and large company users. It also developed an application called 'GOOGLE CLOUD'. And there are also many factors supporting cloud computing like virtualization process, distributed storage, fast and inexpensive server, broadband internet access etc. But the major drawback is security in providing data over the internet. Each and every cloud searcher is raising a question to cloud provider that whether it contains security policies and procedures before hosting their applications. Due to poor security, there exists poor API's, data loss, hijacking, traffic etc. so to protect the data, we proposed RSA algorithm.

Fig 1: *cloud computing architecture*

RSA algorithm is most widely a general purpose approach to public-key encryption. It is an encryption-decryption technique. It consists of plaintext and cipher text in the form of integers between 0 to n-1. This plain text is encrypted in blocks; each and every block has a binary value which should be less than n.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

This algorithm is done in three steps:
Key generation
Encryption
Decryption

II. RELATED WORK

In this paper, degree of uncertainty is justified in cloud computing by using the cipher cloud. It makes the user to make the data in a secured manner on public frameworks. To accomplish this, the encryption process has been carried out (i.e.) user data will be sent to cloud server, and cloud server will send back the data again to the user. The secured data cannot be accessed in the public cloud computing, so to make the data to be private they are using encryption process. [1]

Many companies are using the cloud architectures. Cloud data security depends more on the procedures and count measures. So this paper discusses about the data security issues in cloud. Some of the issues like privacy and confidentiality, data integrity, data allocation and reallocation, data availability, storage and backup recovery etc. to overcome all these type of issues, RSA algorithm has been used. The data will be encrypted and sent to the user, when the user wants the data it will be sent in the decrypted format. [2]

In this paper they discuss about the use of cryptography concepts, to increase the security of encrypted data which is sent by the user to cloud server. The main goal is to encrypt and decrypt the data in a secured way with depletion of less time and less cost in both the encryption and decryption process. Many numbers of keys will be generated and common attacks will be noted. So by repeating the process it helps you to prevent the attacks. [3]

Many of the IT organizations are progressively moving away from device centric views of IT. It is mainly focused on the applications, information, people and all these depend only on the new architecture of cloud computing. In this paper they are discussing about the characteristics of cloud computing and types of clouds, categorization of cloud services, security methods of cloud computing, overview of RSA cryptosystem. [4]

Many of the IT organizations are progressively moving away from device centric views of IT. It is mainly focused on the applications, information, people and all these depend only on the new architecture of cloud computing. In this paper they are discussing about the characteristics of cloud computing and types of clouds, categorization of cloud services, security methods of cloud computing, overview of RSA cryptosystem. [5]

III. PROPOSED WORK

1. RSA Algorithm Process:

RSA algorithm is most widely a general purpose approach to public-key encryption. It is an encryption-decryption technique. It consists of plaintext and cipher text in the form of integers between 0 to n-1. This plain text is encrypted in blocks; each and every block has a binary value which should be less than n.

This algorithm is done in three steps:
Key generation
Encryption
Decryption

The plain text block is taken as M and cipher text block is taken as C. It uses the formula (i.e.) $C=M^e \bmod n$.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

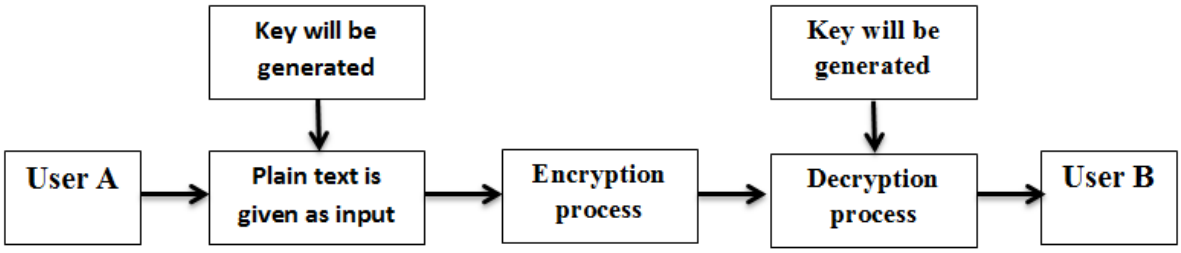

Fig 2: *RSA algorithm structure*

2. Key Generation:

In key generation consider two prime numbers (i.e.) p and q. it consists of public key and a private key. The public key will be known to everyone. Calculate the value of n. select a random encryption key e calculate the gcd and it should be equal to 1. Then find the decryption key d. finally calculate the public key and private key.

The key generation steps are:

Step 1: generate two different primary keys P and Q

Step 2: calculate the modulus n=p*q

Step 3: calculate the $\phi(n) = (p-1) \times (q-1)$

Step 4: select the public exponent an integer e such that $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$

Step 5: calculate the private exponent a value of d such that $d = e^{-1} \bmod \phi(n)$

Step 6: public key = [e,n]

Step 7: private key = [d,n]

Fig 3: *steps in key generation*

3. Encryption process:

In the encryption process represent a plaintext in series of numbers modulo n. the encryption process to obtain ciphertext C from plaintext M is very simple. It is formulated as: $C=M^e \bmod n$

Where C = ciphertext
M = message text
E = public key
D = private key

The file will be encrypted by sending an symmetric file encrypted key (FEK) simultaneously asymmetric public key will generated, both will be combined and forms an encrypted FEK with a header file.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

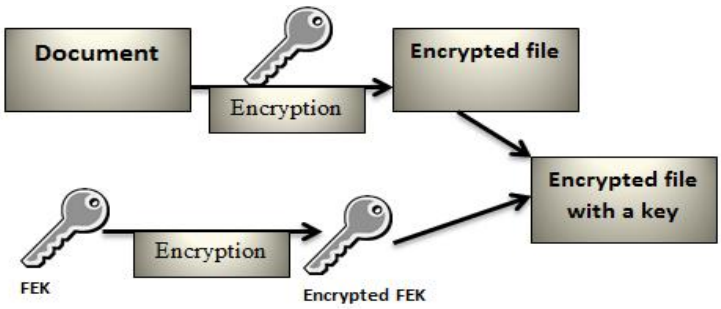

Fig 4: *steps in encryption process*

Decryption process:

The reverse process of encryption will be decryption. It can be generated using the formula: m= e^dmod n.
Where C =ciphertext
M=message text
E =public key
D =private key

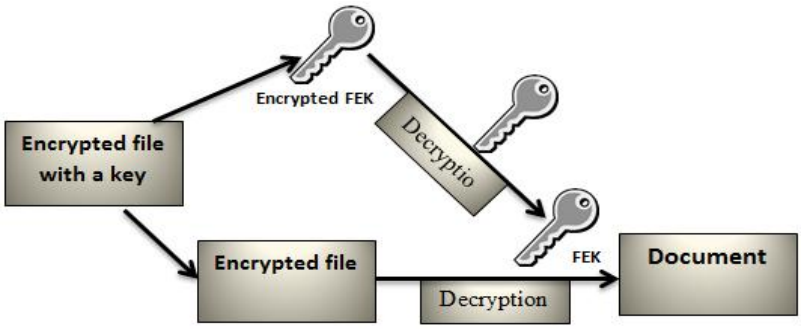

Fig 5: *Decryption process*

IV. EXPERIMENTAL RESULTS

Example for RSA algorithm:

Step 1: Select primes: p=17 &q=11
Step 2: Compute $n = pq$=17×11=187
Step 3: Compute ø(n)=(p–1)(q-1)=16×10=160
Step 4: Select e :gcd(e,160)=1; choose e=7
Step 5: Determine d: de=1 mod 160 and d < 160 Value is d=23 since 23×7=161= 10×160+1
Step 6: Publish public key KU={7,187}
Step 7: Keep secret private key KR={23,17,11}

V. CONCLUSION

RSA algorithm has been implemented and analysed. But the RSA also contains drawback like fake public key algorithm, complexity of key generation, security needs, speed is low. In future work we can use the longer encrypted key with symmetric cipher encryption algorithm key file. It is an excellent method to the symmetric key distribution problem.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

REFERENCES

[1]. ManpreetKaur,Rajbir Singh "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", *International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013*.

[2]. Parsikalpana,Sudhasingaraju" Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication technology,IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[3]. *Anjanachaudhary, ravinder Thakur, manishmann", A review: data security approach in cloud computing by using RSA algorithm",* International Journal of Advance Research in Computer Science and Management Studies, volume 1,Issue 7, December 2013

[4]. SwapnilV.Khedkar , A.D.Gawande*," Data Partitioning Technique to Improve CloudData Storage Security*", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3347-3350

[5]. Ms.ShubhraSaggar, Dr. R.K. Datta"*An improved RSA Encryption Algorithm for Cloud Computing Environments: Two key Generation Encryption (2KGEA)*"ISSN (Online): 2279-0071