ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Data Protection and Reliability in Public Cloud Computing Based on RSA Partial Homomorphic Cryptography

Anjani Kushwaha[1], Prof. Deepak Agrawal[2], Prof. Akshat Khaskalam[3]

Research Scholar, Department of Computer Science & Engineering, Takshshila Institute of Engineering & Technology, Jabalpur [M.P] India[1]

Assistant Professor & Head, Department of Computer & Science Engineering, Takshshila Institute of Engineering & Technology, Jabalpur [M.P] India[2]

Assistant Professor, Takshshila Institute of Engineering & Technology, Jabalpur [M.P] India[3]

ABSTRACT: With the continual advancement in technical field several technologies are evolving day by day, cloud computing is one in all them. With the assistance of cloud computing user will simply share, store and retrieve their knowledge from anyplace. Cloud computing provides hardware, software system and infrastructural storage to several users at a time. As several users share their data on a cloud the most question is concerning security of knowledge gift on cloud.

In this analysis paper answer is provided to keep up knowledge security and data integrity. This theme contains a mixture of RSA Partial homomorphic and MD5 hashing algorithmic program .In this answer knowledge is encrypted by RSA Partial before uploading it on cloud server. when uploading its hash worth is calculated by MD5 hashing theme. All these approaches endure through the following steps Encryption/Decryption, knowledge uploading on a cloud, Hashing and Verification

KEYWORDS: Cloud Computing,; RSA Partial, MD5.

I. INTRODUCTION

Cloud computing is an emerging technology in the field of networking. It is gaining popularity in all areas. The National Institute of Standards and Technology (NIST)[1] defines cloud computing as a model for enabling ubiquitous ,convenient, on demand network access to a shared pool of configurable computing resources. In simple words cloud computing is a computing model in which resources are provided to the users based on their demand. In cloud computing resources are provided by the cloud service provider known as CSP. Many software companies like Google, Microsoft, Amazon, Salesforce, etc. is providing cloud services on different parameter.
By using the services of cloud service provider user's transfer their burden of installing the software, Data maintenance, Infrastructure, Storage space etc. on the cloud service provider. Theses providers offer to their clients the possibility to store, retrieve and share data with other users in a transparent way [2].As data is shared among various users in the cloud there may be possibilities that data may be lostor misuse by other users. It is the biggest matter of concern in cloud computing. Many people afraid to share their data on cloud as they don't know with whom their data is shared.

In this paper a new approach is defined in which firstly the data is encrypted by RSA Partial Homomorphic algorithm and then it is uploaded on cloud servers. In this approach each client can generate their public and private key. In which public key is known to all and private key is only known to the client and authorized users.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

II. LITERATURE REVIEW

NesrineKaaniche et al[2] has proposed ID based cryptography in which the data is firstly encrypted and stored on the public cloud server. This concept also offers access control so that only authorized users can use the data. With the help of this approach unauthorized user even not get the data without client permission.

NehaTirthani et al[3]explain about cloud security issues and then proposed a security model for cloud in which Diffie Hellman Key Exchange and Elliptical Curve Cryptography algorithms are used. The whole model is described in four steps in which first step establish connection, the second is account creation, third is authentication and last step contain data exchange.

FarzadSabahi[4] describe about the scope of migrating to the cloud. The author also explains how the migration to the cloud will benefit to organizations.

Deyan Chen et al.[5] explain some serious security issues with cloud computing and then provide details of current security solution for data security and privacy protection in the cloud.

III. RSA PARTIAL HOMOMORPHIC

This algorithm is named for its developers Rivest, Shamir and Adleman. In 1978 Rivest, Shamir and Adleman invented their public key cryptosystem [6].In RSA Partial Homomorphic method multiplicative homomorphism is used. By multiplying two RSA cipher text together, the decrypted result is equivalent to the multiplication of the two plaintext values.

A. Key Generation

Before encryption of file key is generated. For that the following steps are followed.

- Select two large prime numbers p and q such that

  $p \neq q$.

- Calculate $n=p*q$
- Compute Euler's totientfunction ,$\phi(n)=(p-1)*(q-1)$.
- Choose an integer e such that $1<e<\phi(n)$ and Greatest common divisor(gcd) of e and $\phi(n)$ is 1.This e is public key component.
- Calculate $d = e^{-1} \pmod{\phi(n)}$ i.e. d is multiplicative inverse

  of e modulo $\phi(n)$.

- Now d is take as private key component such that $d*e= 1 \bmod \phi(n)$
- The public key component consists of n and public key component e i.e. (e, n).
- The private key consists of n and private key exponent d i.e. (d, n).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

B. Encryption

$$C=P^e \bmod n$$

Here C is Cipher text, P is plain text and n is the large number and e is a public key component.

C. Decryption

$$P=C^d \bmod n$$

Here all the abbreviations are only one is changed d is a private key component

IV. MD5 HASHING ALGORITHM

MD5 Cryptographic hash calculated function which calculates and output 128 bit hash value. It is also known as message digest algorithm. Basically MD5 uses three operations, which are Bitwise Boolean operation, Modular Addition and Cycle shift operation. For performing MD5 two steps Padding and Compression should be performed.

A. Padding

- In Padding input message is broken up into 512 bit blocks so that input length is divisible by 512. Firstly a single bit is appended at the end of the message. After that a series of 0's are appended so that the length of the padded message is congruent to 448 mod 512.
- This step is followed by adding 64 bit binary string which denotes the length of the message. If the message is very long, greater than 2^{64} then lower 64 bits are used for binary representation.
- **Initialization of the state variable:** In this MD5 uses 4 state variable .The variable is a 32 bit integer. These four variables are sliced and diced. They are named as A,B,C,D and they are having initialization .These initializations are as follows:
  A=0x67452301
  B=0XEFCDAB89
  C=0x98BADCFE D=0x10325476.

B. Compression

- Now the algorithm uses four functions. These functions are as follows.
  F(X, Y, Z) =(X&Y) | ((~X)&Z) G(X, Y, Z) =(X&Z) | (Y& (~Z)) H(X, Y, Z) =X^Y^Z
  I(X, Y, Z) =Y ^ (X|~ (Z))

Here **&,** | , ^ , ~ are bitwise AND, OR, XOR and NOT operator. For each 512 bits this round is performed. After this step the result which is in the message digest form is stored in the state variable A, B, C, D.

V. PROPOSED MODEL

In this model three major entities Data owner, CSP and User are the main entity. Data owner are the person who uploads their data, User are the persons who request for the data and CSP are cloud service provider who provide a cloud environment for the whole model .The steps of the proposed model are as follows:

A. Proposed Work

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

In the proposed work for keeping the data secure firstly the data is encrypted with the RSA homomorphic algorithm after that public and private key related with file is generated. As encryptions are performed file is ready to be uploaded on cloud servers. After uploading Data owner gets its general detail like uploading time, date, hash generation of file and verification. In this approach for maintaining data security access permission to the specified file is defined. Specified user get the file in encrypted form which can be decrypted by a private key which was generated at the time of encryption. In case if any, malicious get the data they are not able to decrypt it.

B. Prerequisites

Before uploading the file on cloud some basic steps have to be done which is encrypted of the specified file and generation of public and private key. In this model for encryption , RSA partial homomorphic algorithm is used. For encryption user has to only upload their file and then generate its public key. After a generation of public key its related private key is also generated which is used for secure communication. Now the encrypted file is further sent to the cloud server for uploading. The access file is also uploaded at the time of decryption which contains details of authorized users.

C. Secure Data Storage

As Data owner upload their file on cloud they get general detail of files like uploading date, time , etc. Some other steps are also performed which are as follows:

x *Secure Data Backup*

As data or file is uploaded on cloud it is necessary to keep this data secure for future usage so that the data cannot be damaged or lost. For keeping the data backup strong the following steps should be performed:

A. Hashing

For keeping the data secure on the cloud hash value of the uploaded file is calculated. This hashing is performed by Cloud Service Provider with the help of the MD5 hashing algorithm. A copy of calculating hash value is send to the data owner which is further used for verification purpose. Hence on Cloud Service Provider only encrypted data with its hash value is present, which is beneficial for security purpose because the cloud service provider does not use it for malicious purpose.

B. Verification

Verification is an important domain of this model. In this part data present on cloud is verified by data owner just to check data integrity. This task is performed at cloud server end. As described in the previous section after calculation of the hash value of the uploaded data its value is returned back to the data owner. In future data owner can verify their data by requesting for verification option. As owner requests for this option hash value of the data present at cloud is calculated. This calculated hash value is matches with the old hash value which is present at owner end. If this value match's then data present at the cloud is safe and no modification has been done if it does not match then there are some changes on cloud data. The Owner gets the output in the form of a report.

D. Secure Data sharing

The data sharing process in which data owner share their data with users. For sharing user access list should be generated by the owner. This access list is previously generated which contain the names of authorized users. For secured communication private key is sent through email to the users. In this approach , each other's access permit is hidden with each others. The access permission is in two forms Read Only and Read and Write. Their description is as follows:

x *Read Only*: The user with this permission can only read the data; they cannot make any modification on it.
x *Read and Write*: The users with this permission can perform both Read and Write operations on the file.
In this way data security is maintained.

VI. IMPLEMENTATION RESULT

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

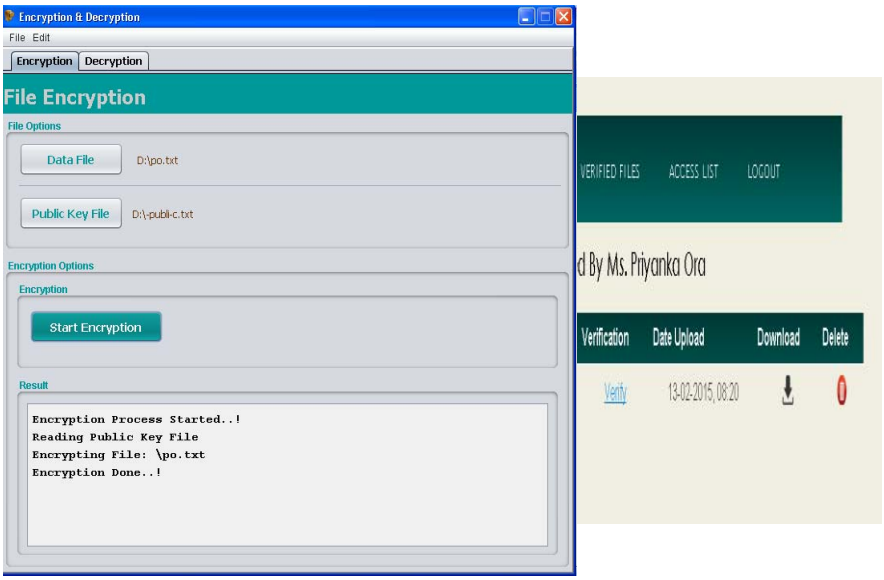
Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

The whole model is implemented on a public cloud. In this model for cloud environment Openshift public cloud is used. For coding Eclipse Kepler version and the JDK 1.6 version is used. Some important snapshots are as follows.

A. Encryption

In this form the first process of the model , i.e. generation of public key and private key through encryption and decryption of file is done. In this process Data Owner simple upload their file followed by its public key. Here Public key work as an identity of Owner at cloud server. This form encrypts the file and generate private key as an output. download the encrypted file and in Delete owner can delete the uploaded file.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

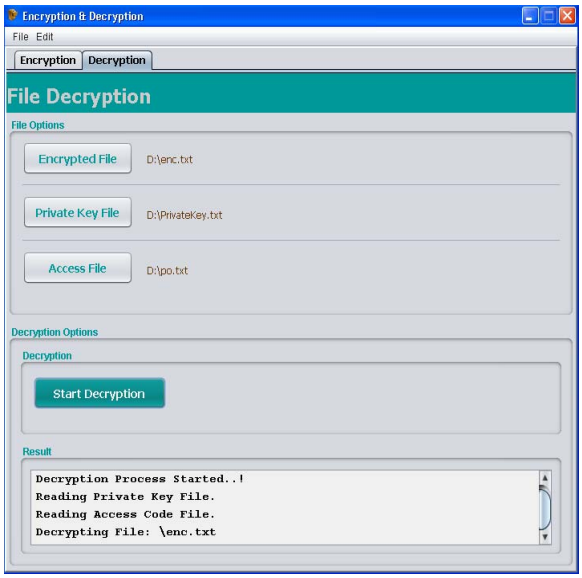
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

B. Decryption

This form Decrypt the file with the help of private key. This form also needs access list of authenticated users.

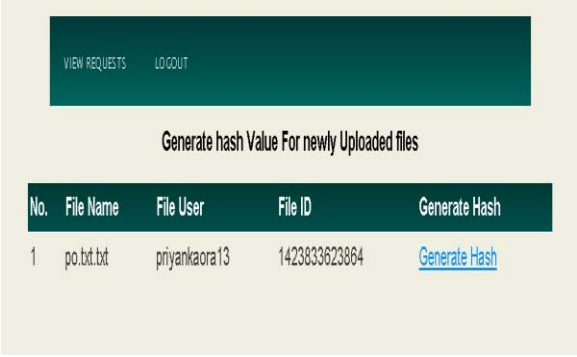


C. Data Uploaded On Cloud Server

After encryption Owner simply upload encrypted files on openshift public cloud. After uploading owner get general details like file name, size, uploaded date and time, Hash value generation and verification. In downloading user can

D. Hash Value Generation

After uploading the file on cloud its hash value is calculated. This calculated hash value is sent to the data owner for backup purpose. The hash value is calculated at cloud server end.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

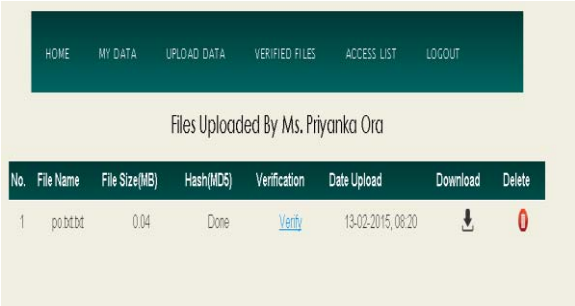
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

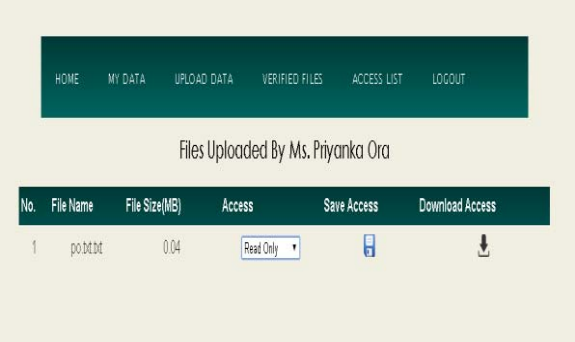
Vol. 7, Issue 1, January 2019

After generation it gives notification of hashing completion.



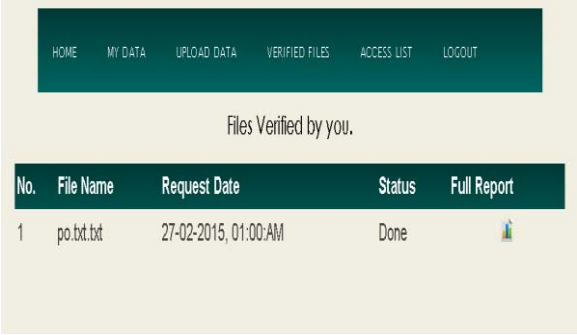
E. Access Permission

On the uploaded file two access permissions Read only and Read and Write only is defined. After defining permissions , owner saves this access permission and confirm its permissions.



F. Verification

For secure backup of the data verification is needed to be performed. For that owner verify specified file and then get a report which contain verification result.



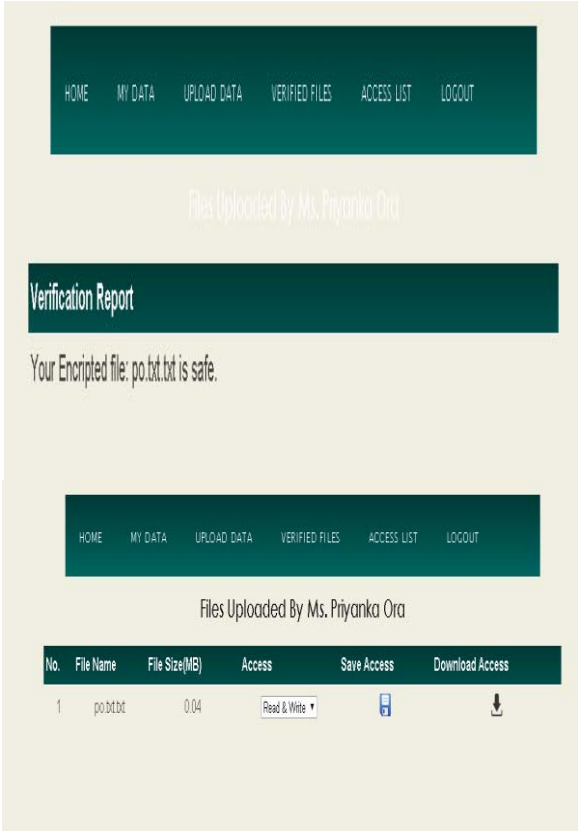
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019



VI. SECURITY DISCUSSION

In this section an informal security discussion is proposed which are as follows.

A. Confidentiality

In this proposal encryption is performed for data confidentiality. Firstly the data is encrypted with RSA Partial homomorphic which results in generation of public and private key. This encrypted file is then uploaded on cloud servers. In case if any, malicious get the data they are not able to get the original data as they don't have a private key. In this manner data is kept confidential with other users.

B. Access control

For secure sharing of data twofold mechanism is used. One is access permission on the file is granted by owner and managed by cloud server provider. If any user wants to access data their identity must be authenticated by CSP. The second is even though any malicious gain access on cloud they can download the data, but they don't have the private key to decrypt it. In this way security of data is maintained.

C. Integrity

It is the most important approach uploaded data cannot be modified by other users. As Data owner can perform verification at any time. In this approach hash value of the data present at cloud and present at the owner end is matched. If this values matches, then data is safe if it does not match, then modification has been done on the data. In

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

this way the owner is having hold on their data, they can easily verify it. CSP also control the things very wisely as control of the data is provided by the owner .In this way the integrity of the data is maintained.

VII. CONCLUSION

In this paper a solution is proposed to maintain data security and data integrity on cloud servers. For this approach RSA partial homomorphic and MD5 hashing algorithm is used. Encryption and decryption is done by RSA partial algorithm,whereas MD5 hashing algorithm is used for secure data backup.

With future emphasis is given to implement the proposed architecture with different comparison to show the effectiveness of our approach.

REFERENCES

1. P.Mell and T.Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology,Vol.53,no.6,p.50,2009. [Online]. Available:* http://csrc.nist.gov/groups/SNS/cloud computing/clouddefv15.doc.
2. NesrineKaaniche,AymenBoudguiga, Maryline Laurent, "ID Based Cryptography for Secure Cloud Data Storage,"Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference .
3. NehaTirthani, GanesanR,"Data Security in Cloud Architecture Based on diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research, Nov 2013.
4. FarzadSabahi,"Cloud computing Security threats and responses "Communication Software and Networks(ICCSN).2011 IEEE 3rd International Conference.
5. DeyanChen,Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing, " 2012 IEEE International Conference on Computer and Electronics engineering.
6. Ronald L. Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of ACM*, 21(2):120{126, February 1978.