INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
(Volume2, Issue5)
Available online at: www.Ijariit.com

Review on Encrypt the text by MD5 and RSA in Client Cloud Approach

Adviti Chauhan[1]
Electronics and Communication & HPTU
advitichauhan@gmail.com

Jyoti Gupta[2]
Faculty of Electronics and Communication & HPTU
Jyotigpta5@gmail.com

Abstract*— *Cloud computing is one of the emerging technology which is showing continuous advancement in the field of networking. Cloud computing is defined by National Institute of Standards and Technology (NIST)[1] as a model for enabling ubiquitous, on demand network access to a shared pool of configuration computing resources (e.g. computer networks, servers, storage, applications and services) ,which can be rapidly provisioned and release with minimal management effort. It is gaining popularity in all the areas. But still by far cloud computing sharing is behind one expected because of the security concerns (unauthorized access, modification or denial of services, etc). In this research paper, the proposed work plan is to eliminate security concerns using cryptographic algorithm and hashing algorithm.

Keywords— Cloud computing, RSA partial, MD5, CSP.

I. INTRODUCTION

With the rapid growth in the need for computing resources and advancement in networking technology have prompted many organisation to outsource new economic and computing model referred to as cloud computing. The customers can avoid the cost of building and maintaining a private storage infrastructure by moving data to the cloud and have function of it needs by paying a service provider. Cloud service provider referred as CSP, provides cloud computing resources. With the use of services provided by the cloud service provider, the burden of software installation, storage space, data management, etc. is transferred on cloud service provider and provides some other benefits including

- Availability (i.e. data can be accessed from anywhere)
- Reliability (i.e. having backups)

Cloud service provider offers a transparent way to store, retrieve, and share data with user's [5].
Unfortunately, several security concerns are there in cloud computing. Security concerns including

- Data breaches(i.e. unauthorized data access)
- Data loss(i.e. disk drive dies before the data backup is created)
- Data ownership(i.e. denial of service)

Because of these security concerns, many organisations are still afraid to share their data on cloud.
In this paper solution for these security concerns are provided by using RSA partial homomorphic and MD5 hashing algorithm. Before uploading the data on the on cloud server, RSA partial homomorphic algorithm is used to encrypt the data. MD5 hashing algorithm is used to calculate its hash value after the data is uploaded on client server.

II. LITERATURE REVIEW

Shakeeba S. Khan et.al.[2] has proposed Multilevel cryptographic algorithm which will provide more security for cloud computing than using single level encryption. The cryptographic algorithms proposed in this paper are DES algorithm and RSA algorithm.

Priyanka Ora et.al.[3] has proposed a scheme for maintaining data security and data integrity by using combination of RSA partial homomorphic and MD5 hashing algorithm. Encryption and decryption id done by RSA partial algorithm, whereas MD5 hashing algorithm is used for secure data backup.

Neha Tirthani et.al.[4]explains some cloud security concerns and then proposed a model which uses Diffie Hellman Key Exchange and Elliptical Curve Cryptography algorithm. The whole model is a four step method

- Establish connection
- Account creation
- Authentication
- Data exchange

Nesrine Kaaniche et.al[5] describes the security issues in cloud storage service and proposed an ID-Based Cryptographic scheme which offers access control so that only authorized user can access the data.

Seny Kamara et.al[6] gives an overview of recent advances in cryptography motivated specifically by cloud storage. This paper describes several architecture that combines recent and non-standard cryptographic primitives in order to build a secure cloud storage service.

Deyan Chen et.al[7]explains some serious security issues with cloud computing and provide details of current security solution and future scope for data security and privacy protection issues in the cloud.

III. CRYPTOGRAPHIC ALGORITHM AND HASHING ALGORITHM

There are number of techniques used to implement security in cloud computing. Some of the existing algorithms implemented are as follows:

A. RSA Partial Homomorphic Algorithm

This algorithm was developed by Rivest, Shamir, and Adleman in 1977. RSA is an algorithm based on a property of positive integers which uses modular exponential for encryption and decryption. It is an asymmetric key cryptographic algorithm. It involves a public key and a private key. The public key is used to encrypt the message and is known to everyone. RSA partial homomorphic algorithm uses multiplicative homomorphism. The encrypted result is the multiple of two RSA cipher text and the multiple of two plain text is the decryption result. The message can only be decrypted by private key. Basic three processes that RSA algorithm go through are

- Key generation
- Encryption
- Decryption

Key is generated before the encryption process. Following steps are followed for key generation.

1. p, q, two prime numbers.

   (private, chosen)
2. n=pq

   (public, calculated)
3. φ(n)=(p-1)(q-1)

   (private, calculated)
4. e, with gcd(φ(n),e)=1; 1<e<φ(n)

   (public, chosen)
5. d=e^{-1}mod φ(n)

   (private, calculated)

The public key component consist of n and public key component e i.e. (e, n). The private key component consist of n and public key exponent d i.e. (d, n).

Encryption and decryption are of the following form, for some plaintext block P and cipher text block C:

C=P^emod n

P=C^dmod n

Here C is the cipher text. P is plain text. Where n is the large number, e is a public key component and d is the private key component.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

B. MD5 Hashing Algorithm

The MD5 message-digest algorithm widely used for secure hash algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit message digest. The input is processed in 512-bit blocks. The process consists of following process:

- Append padding bits

The message is padded so that its length in bits is congruent to 448 modulo 512. That is, the length of the padded message is 64 bits less than an integer multiple of 512 bits.

- Append length

If the original message is greater than 2^{64}, then only the low-order 64 bits of the length are used.

- Initialize MD buffer

A 128-bit buffer is used to hold intermediate and final results of the hash function. These 32-bit registers are initialize to the following 32-bit integers.
A=67452301
B=EFCDAB89
C=98BADCFE
D=10325476
These values are stored in little-endian format.
wordA: 01 23 45 67
wordB: 89 AB CD EF
wordC: FE DC BA 98
wordD: 76 54 32 10

- MD5 compression function

The processing of the 512-bit block in four rounds. Each round consists of a sequence of 16 steps operation on the buffer ABCD.
The function can be summarized as follows:

Round	**Primitive function g**	**g(b,c,d)**
1	F(b, c, d)	$(b \wedge c) \vee (\bar{b} \wedge d)$
2	G(b, c, d)	$(b \wedge d) \vee (c \wedge \bar{d})$
3	H(b, c, d)	$b \oplus c \oplus d$
4	I(b, c, d)	$c \oplus (b \vee \bar{d})$

Figure 1

The logical operators (AND, OR, NOT, XOR) are represented by the symbols ($\vee$, $\wedge$, $\bar{}$, $\oplus$).[12] After this round is performed on 512 bits, the result is stored in the state variable A, B, C, D.

IV. REVIEW MODEL

A. System Design

This scheme uses RSA partial homomorphic algorithm for encryption before uploading the data in cloud server. After the data is being uploading, MD5 hashing algorithm is used to generate hash value.
The proposed system design focuses on the following objectives which are helpful in increasing the security of the stored data.

1. Encryption

1) First, RSA partial homomorphic algorithm is used to encrypt the data and to generate private and public key.
2) The encrypted file is then uploaded to the cloud servers.
3) General details like uploading details (time, date), hashing generation of file and verification details are obtained by data owner.
4) User can only be able to decrypt the data by using private key, generated during data encryption.
5) If data gets malicious, then data will not be decrypted.
6) Detail of authorized users in an access file is also uploading at the time of decryption.

2. Hashing and verification

1) Cloud service provider performs hashing by using MD5 hashing algorithm.
2) The hash value is also send to the data owner which can be used for verification purpose.
3) The data owner can request for verification and to verify, hash value is generated of the present value present at the cloud.
4) To verify the old hash value which is present at the owner end with the hash value generated?
5) For secure data access, the list of user is generated by the data owner.

6) The private key is sent to the user through email for secure communication.
7) There are two forms of access provided by the data owner to the user.
   a) Read only
   b) Read and write

By the use of this proposed scheme, data security concerns are being maintained.

B. Algorithm

We proposed a combination of security algorithms to eliminate security concerns. The two security algorithm used are RSA partial homomorphic algorithm and MD5 hashing algorithm. RSA is asymmetric key algorithm that uses different keys for encryption and decryption. RSA partial homomorphic algorithm uses multiplicative homomorphism. The encryption result is multiple of two RSA cipher text and decryption result is multiple of two plain text. Whereas MD5 algorithm is used to calculate the hash value after the encrypted data is uploaded in the cloud. The block diagram of the RSA partial homomorphic encryption algorithm and MD5 hashing algorithm is shown in following figure 2.

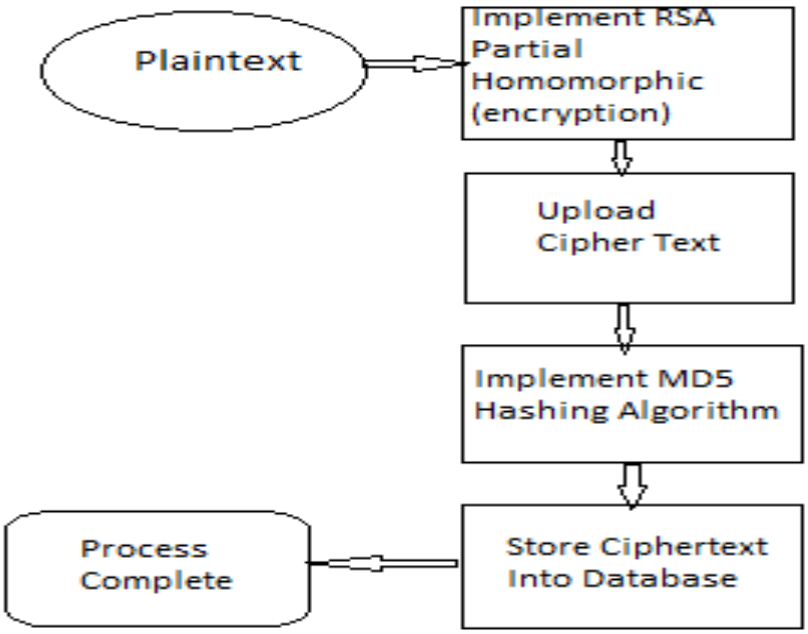

Figure 2.

As shown in figure 2, the steps for the encryption algorithm and hashing algorithm will be as follows:

- Plaintext is converted into cipher text by implementing RSA partial homomorphic algorithm.
- Two keys are generated, public key and private key. The private key is sent to the user through email for secure communication.
- The encrypted file is then uploaded to the cloud servers.
- General uploading details are obtained by the data owner.
- Then, MD5 hashing algorithm is used to generate hash value for verification purpose.
- After the completion of hashing function, it will be stored in Database of cloud for backup purpose.

When the data is being downloaded, inverse of RSA partial homomorphic algorithm is used to decrypt data. . The block diagram of the RSA partial homomorphic decryption algorithm and MD5 hashing algorithm is shown in following figure 3.

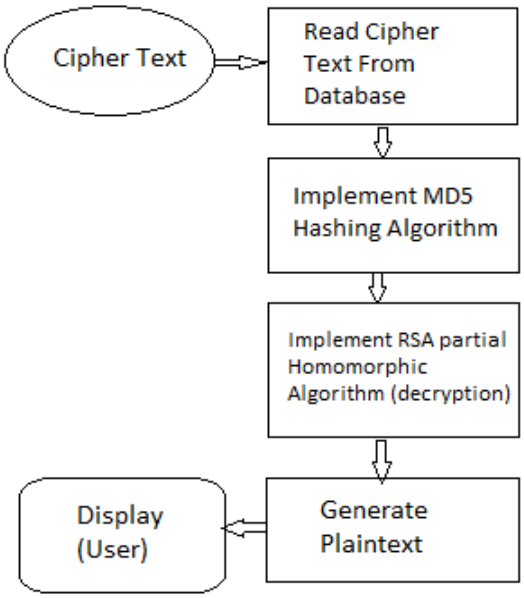

Figure 3.

As shown in the figure 3, the steps for decryption algorithm and hashing verification function will be as follows:

- To decrypt the data, inverse RSA partial homomorphic algorithm is used.
- The data owner can request for verification and to verify, hash value is generated of the data value present at the cloud.
- To verify the old hash value which is present at the owner end with the hash value generated?
- If the value does not match that means data has been modified. So the CSP does not decrypt the data but instead the output displayed is in the form of a report.
- If the hash value generated matches, data is safe and no modifications have been done.
- Then the data is decrypted by using RSA partial homomorphic algorithm and the plaintext is displayed to the user.

V. CONCLUSIONS

In this paper cryptographic algorithm and hashing algorithm is used to eliminate security concerns (unauthorized access, modification, etc). For encryption and decryption of the data RSA partial homomorphic algorithm is used for access control. For the verification, data backup and hashing function, MD5 hashing algorithm is used after the data is being uploaded on the cloud.

With future emphasis given to the cloud computing security concerns, we believe that many research problems are remain to be eliminated.

SR. NO.	AUTHOR NAME	YEAR	TECHNOLOGY USED	DESCRIPTION
1.	Peter Mell Timothy Grance	2011	Cloud Computing	The NIST definition describes an important aspect of cloud computing. For best use of cloud computing, it serve as a mean for broad comparisons of cloud services and deployment strategies.
2.	Shakeeba S. Khan Prof. R.R. Tuteja	2015	Multilevel Encryption and Decryption Algorithm	Using multilevel cryptographic algorithm to enhance the security in cloud as per different perspective of cloud customer.
3.	Priyanka Ora Dr. P.R. Pal	2015	RSA partial homomorphic and MD5 Cryptography	To maintain data security and data integrity, combination of RSA partial homomorphic and MD5 hashing algorithm is used.

4.	Neha Tirthani Ganesan R	2014	Diffie Hellman and Elliptical Curve Cryptography	The non-breakability of Elliptical curve cryptography for data encryption and Diffie Hellman Key exchange mechanism for connection establishment is used which ensures the secure movement of data at client and server end.
5.	Nesrine Kaaniche Aymen Boudguiga Maryline Laurent	2013	ID-Based Cryptography	For secure cloud storage services and controlled data access, the proposed cryptographic scheme is ID-Based cryptography.
6.	Seny Kamara Kristin Lauter	2010	Cloud Computing, Cryptography	For secure cloud storage, combination of recent and non- standard cryptographic primitives are described.
7.	Deyan Chen Hong Zhao	2012	Cloud Computing	Describes all-round analysis on data security and privacy protection issues associated with cloud computing.
8.	A.L. Jeeva Dr. V. Palanisamy K. Kanagaram	2012	Cryptography, Symmetric Key Encryption and Asymmetric Key Encryption	A fair comparison between the various cryptographic algorithm to provide a better solution for data confidentiality and privacy.
9.	Randeep Kaur Supriya Kinger	2014	Cloud Computing, Security Algorithm	Explains number of existing security algorithm used to provide security in the field of cloud computing.
10.	Maha Tebaa Said El Haji Abdellatif El Ghazi	2012	Cloud Computing, Homomorphic Encryption	The cloud computing based security based on fully homomorphic encryption, which ensure the data confidentiality by enabling the operation on encrypted raw data.
11.	Lori M. Kaufman	2009	Cloud Computing	Describes the cloud computing environment, the industry itself should establish coherent and effective policy and governance to identify and implement proper security methods.

REFERENCES

1. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
2. Khan, M. S. S., & Deshmukh, M. S. S. (2014). Security in Cloud Computing Using Cryptographic Algorithms.
3. Ora, P., & Pal, P. R. (2015, September). Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography. In *Computer, Communication and Control (IC4), 2015 International Conference on* (pp. 1-6). IEEE.
4. Tirthani, N., & Ganesan, R. (2014). Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. *IACR Cryptology ePrint Archive*, *2014*, 49.
5. Kaaniche, N., Boudguiga, A., & Laurent, M. (2013, June). ID based cryptography for secure cloud data storage. In *CLOUD 2013: IEEE 6th International Conference on Cloud Computing* (pp. 375-382). IEEE.
6. Kamara, S., & Lauter, K. (2010, January). Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security* (pp. 136-149). Springer Berlin Heidelberg.
7. Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651). IEEE.

8. Jeeva, A. L., Palanisamy, D. V., & Kanagaram, K. (2012). Comparative analysis of performance efficiency and security measures of some encryption algorithms. *International Journal of Engineering Research and Applications (IJERA) ISSN*, 2248-9622.
9. Kaur, R., & Kinger, S. (2014). Analysis of security algorithms in cloud computing. *International Journal of Application or Innovation in Engineering and Management*, *3*(3), 171-6.
10. Tebaa, M., El Hajji, S., & El Ghazi, A. (2012, July). Homomorphic encryption applied to the cloud computing security. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 4-6).
11. Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy*, *7*(4), 61-64.
12. Stallings, W. (2006). *Cryptography and network security: principles and practices*. Pearson Education India.

