IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Protected File Storage on Cloud Using Cryptography

Vidyashree Akhouri* and Dr. Javed Wasim**

*Research Scholar, Department of Computer Science and Technology Engineering & Applications, Mangalayatan University, Aligarh

**Assistant Professor-II, Department of Computer Science and Technology Engineering & Applications, Mangalayatan University, Aligarh

ABSTRACT

Cryptography is the study of the various process which are implemented to protect information and communications, through the use of mathematical concepts and rule-based calculations but intruder is able to read our data so we need some method to make this data unreadable by the intruder we do this by encryption (enciphering) is a cryptographic process where we convert plain text or raw data to unintelligible information (cipher) by processing the data with an algorithm . Decryption (deciphering)is a cryptographic process where we convert cipher back to plaintext by processing. the encryption and decryption techniques that we are using should be fast in nature so when it reaches the recipient, the recipient should be able to decrypt that data fast because time is extremely valuable and the recipient cannot sit and decrypt that data for one to two hours it should be decrypted in minutes.

Aim of this paper is to use different cryptography algorithm to protect file stored on cloud.

The present paper involves some security goals in the process of cryptography we need to absolutely protect the confidentiality of the data so cryptography is the study that helps us deal with that it protect the confidentiality of data , when we are implementing cryptography that means there exist confidentiality.

Second goal is integrity means that the data should have its original meaning should have its original structure when it reaches the recipient so if we write something in beginning right and u convert it into cipher ,when we send the cipher over to the recipient and the recipient deciphers it converts it back into plain text the plain text should represent exactly what the sender sent in the first place so the data should have maintained its integrity. Third is availability it means that the people who require that data should have it basically instantly right they should not have any delay with getting that nobody should be able to interrupt to the process of them getting that data right so this particular aspect is called availability.

So this another goal of cryptography to maintain integrity to secure and strongly store information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality, integrity and ensures availability.

For this purpose we searched different published research articles online on cloud cryptography algorithm. Published research articles were selected from IEEE and Springer nature journals. Total seven articles between the years 2010 to 2021 were taken for the purpose of present paper. Our methodology guarantees the security and protection of customer sensitive data by utilizing AES, DES and RC2 calculation. By using all the encryption techniques a fair unit of confidentiality, authentication, integrity, access control and availability of data is maintained. Using cryptography Electronic Mail Security, Mail Security, IP Security, Web Security can be achieved.

Key words: cryptography, Algorithm, AES, DESB

INTRODUCTION

Cryptology is the study of converting plain text to cipher text and vice-versa. So it is the study of both encryption and decryption. It is done on both the sides sender and receiver. Basically we find two types of cryptography first is private key cryptography it involves single key for whole process. Private key cryptography (symmetric key cryptography) uses a single common key on the receiving and sending end. Second is public key cryptography it involves two keys so public key cryptography (Asymmetric key Cryptography) uses a non secretive public key for encryption , and a secretive private key for decryption.

Cryptography is the protecting technique of data from the unauthorized party by converting into the non-readable form. The main purpose of cryptography is maintaining the security of the data from third party. There are following two types of algorithms such as: (i) symmetric key based algorithm, sometimes known as conventional key algorithm and (ii) asymmetric key based algorithm, also known as public-key algorithm.
In this paper we found that Advance Encryption Standard (AES), Data Encryption Standard (DES) and Ron's Code or Rivest Cipher (RC2) are important cryptography algorithm to save and maintain confidentiality of the save file on cloud. The AES algorithm has own particular structure to encrypt and decrypt sensitive data. This algorithm is applied in hardware and software all over the world. AES is the ability to deal with three different key sizes such as AES 128,192 and 256 and each of this ciphers has 128 bits block size (Ako Muhammad Abdulla
h, June 2017).Whereas DES is a block cipher and encrypts data in block of size of 64 bit each. That means 64 bits of plain text goes as the input to DES which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption with minor differences (https://www.geeksforgeeks.org). In cryptography a conventional (secret-key) block encryption algorithm called RC2 which may be considered as a proposal for a DES replacement. The input and output block sizes are 64 bits each. The key size is variable from 1 byte up to 128 bytes, although the current implementation uses eight bytes (https://www.ipa.go.jp).

RSA algorithm maintains all three objectives that is confidentiality,integrity and availability for protecting file storage in cloud . So now we will discuss RSA algorithm .

RSA ALGORITHM (Rivest,Shamir,Adlemann)

We chooses two large prime numbers p and q such that

$$P \neq Q .$$

Then we have to compute

$n = P*Q$.

$\emptyset(n)= \emptyset(p*q) = \emptyset(p) *\emptyset(q)$

$=(p-1)(q-1)$ [By Euler's Totient Function]

Now we choose 'e'; $1\leq e \leq \emptyset(n)$, co prime to $\{\emptyset(n),e\}$

(e,n) = public key

We have to determine 'd' as $ed = 1 \bmod \emptyset(n)$

$d = e^{-1} \bmod Ø(n)$; (d is multiplicative inverse of e)

[d= (Ø(n)*i) + 1/e] [where i=1,2,3,4,5.....]

(d,n) = private key

Example→

Suppose there are two different users A and B

A—(5)-(PLAIN TEXT)----------B

P=7, Q=11

n = 7*11 = 77

Also we have,

Ø(n) = Ø(p*q) = Ø(p)*Ø(q)

(p-1)(q-1)= (7-1)(11-1)=6*10=60

Ø(n) = 60

Choose e =13 which is $1 \leq e \leq Ø(n)$

Public key = (13 , 77)

Now,

We have find out the value of d

$d = e^{-1} \bmod Ø(n)$ (We can find the value of D by using multiplicative inverse)

13 * d= 1 mod 60

The value of d should be 37.

D=Private key=(37,77)

$C.T.= (P.T)^{E} \bmod N$

$C.T.= (5)^{13} \bmod 77$

(After solving this equation we will get)

C.T.=26

$(P.T) = (C.T)^{D} \bmod N$

$P.T.= (26)^{37} \bmod 77$

P.T.= 5

Finally B Will get the plain text 5 which A has sent.

RESEARCH GAPS

Research gap	Short coming	Reference
Without RSA Algorithm the high secure and high potential data is impossible.	Along with implementation of RSA algorithm,the author has described the performance of Time Complexity, Space Complexity and Throughput . Even then the Cloud Computing has many challenges for data security. **Security of the Cloud relies on trusted computing and cryptography..**	Santosh kumar Singh et. al (2016), JARCCE Data Security using RSA Algorithm in Cloud Computing. Dr. Rajamohan et. al (2019), Proposed hybrid RSA algorithm for cloud computing,
No solution for confidentiality is found	Author has tried to attribute the quality of two cryptographic mechanisms, namely, Symmetric Key and Asymmetric Key algorithms as well as RSA algorithm but no sure solution of Confidentiality was found.	George Amalarethinam H.M. Leena ,(2016) Enhanced RSA algorithm for data security in cloud.
Lack of huge potential and promising innovations.	The author has pointed out that the fault – tolerance, reliability and load balancing is still a hindrance in the adoption of cloud security.	Rohini; Tejinder Sharma (2018) Proposed hybrid RSA algorithm for cloud computing
It has several limitations and time consuming nature while migrating between VMs.	Author talks about virtualization in cloud computing, this helps the business providers and industries to increase their productivity	Algorithm R. Thilagavathy and A. Murugan , Dr. Ambedkar Indian Journal of Science and Technology, Secure the Cloud Data Transmission using an Improved RSA
No permanent algorithm solutions for confidentiality, integrity and authentication	In this model authors have implemented a combination of RSA encryption and digital signature technique	International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014 ISSN: 2347-8578 www.ijcstjournal.org Page 60 Enhancing Data Security in Cloud Computing Using RSA Encryption .

Data security issues in Protected File Storage on Cloud -→

The main issues related to cloud computing is security. As there is always threat of hacking of data .It is the main concerned of customer to protect its data from the unauthorized person as there is always risk of data hacking .So there are many issues related to security which comprises both concerns and threats.

Security concerns:

i) Third party handling data- Third party accessing and managing the data and also no guarantee (100%) about data security.

ii) Cyber attacks-One of the top challenging issues.

iii) Insider threat-Privacy of data.

iv) Govt. intrusion-Super vision of data , keep survillence type of system to monitor the data, it is never say that ur data is completely to your data ,.

v) Legal liability-There can be court case filed against you or by you.

vi) Lack of support every company how much support provide there consumers, there is a competition going

vii) Lack Of Standardization - different cloud suppliers may not follow always same standards.

Threats:

i) DOS-Denial Of Service - Tries to bring server down means flooding of network or legitimate request stop to serve.

ii) MIM- Man In The Middle- Communication of two parties is not secure means litens communication between client and cloud.

iii) NS-Network Sniffing- it si basically monitoring all the traffic in the network.

IV) PS-Port Scanning –Hackers tries to steal about ports used.

v) SIA-Sql Injection Attack- It is a very dangerous attack means direct database attack , hakers tries to to steal Credentials from database.

vi) XSS-Cross Site Scripting - Hackers embedding harmful links or script.

File Storage

Stages of a Cloud Journey

A cloud journey is not just a technical change. It involves changes to the entire IT framework, multiple business departments, and critical business processes. Translating business goals into a migration plan is time consuming, but advanced planning is key to a successful migration. The following steps present a framework for planning and executing your cloud vision.

- Step One: First we have to make the Business Case. A cloud journey is a business decision.
    - There is essential to understand the difference between cloud and traditional IT setup. They must be able to judge the benefits, risks, compliance, security, and data control implications on the organization as a whole and its IT activities.

- ...
- Step Two: We should identify the right applications for file storage. It is not ecessary for each application to fit in the cloud environment.So the application should be suitable for the cloud so that it can just fit and shift according to the cloud.

Step Three: When we select a Cloud Service Provider ,the cloud provider offers a distinct architecture that can with a unique set of capabilities, licensing, and support. For assessing a cloud provider we must ask several questions –

Does the architecture of the cloud go with the design of our workloads?

What kind of cloud implementation is supported by the provider?

Can you bring your own existing licensing to the cloud?

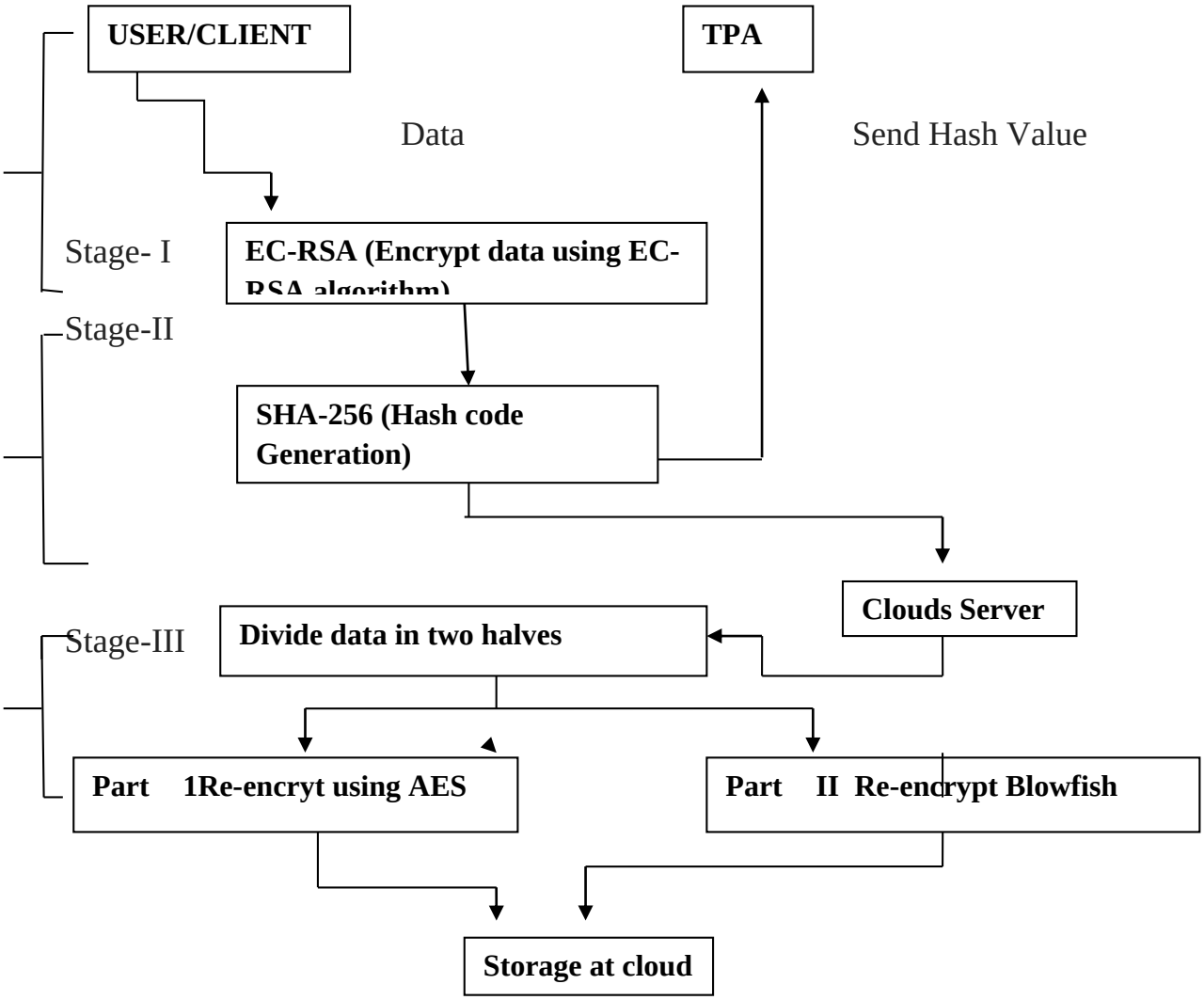
What type of support do you need before, during, and after the migration process?

There are many more aspects like security, compliance, and service level agreements to consider when migrating to the cloud.

- Step Four: Initial Adoption The first and simplest solution adopted by companies migrating to the cloud IS Software as a service (SaaS).

Step Five: Full Migration includes testing because it **is** a huge part of the execution. First we should test our plan, and then start executing it. We should create a backup and recovery strategy, and use it if or when issues occur.

- Step Six: Post-Migration. For completing our journey it is the time to begin comparing pre- and post-migration performance. . Now we should monitor cloud performance on the basis of our provider's service level agreements (SLAs) and our own performance goals.



CONCLUSIONS AND FUTURE WORK

This study shows that using prime numbers in public key cryptography algorithms leads to increased security. The proposed algorithm RSA has been implemented in such a way that it creates not only a complex calculation but the speed of encryption and decryption time with the help of two different end values .It is observed that when the file size is increased there is a little change in the decryption time. The main goal is to securely store and access data in the cloud that does not control ownership of the data. Storing and accessing data is more secure and has some high performance. We have ongoing efforts to address the problem of group simplification of data in the shared likes section because in this scheme only the member of the group can access the data . One to many ,many to one and many to many communication is not possible. In future, the Chinese Remainder Theorem can be applied in decryption process.

REFERENCE

Santosh kumar Singh et. al (2016), JARCCE Data Security using RSA Algorithm in Cloud Computing. International Journal of Advanced Research in Computer and Communication Engineering. Vol. 5, Issue 8.

1. Dr. Rajamohan et. al (2019), Proposed hybrid RSA algorithm for cloud computing, International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4.
2. George Amalarethinam H.M. Leena , (2016) Enhanced RSA algorithm for data security in cloud.
3. Rohini; Tejinder Sharma (2018) Proposed hybrid RSA algorithm for cloud computing
4. Algorithm R. Thilagavathy and A. Murugan , Dr. Ambedkar Indian Journal of Science and Technology, Secure the Cloud Data Transmission using an Improved RSA
5. International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014 ISSN: 2347-8578 www.ijcstjournal.org Page 60 Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm Sudhansu Ranjan Lenka , Biswaranjan Nayak Department of Computer Science and Engineering , Trident Academy of Technology
6. International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 03 | Mar-2018 PROTECTED FILE STORAGE ON CLOUD USING CRYPTOGRAPHY
7. https://doi.org/10.14778/2367502.2367572
8. IEEE Transactions on Knowledge and Data Engineering (Volume: 26, Issue: 1, Jan. 2014) Page(s): 97 - 107
   Date of Publication: 26 June 2013 ISSN Information: Publisher: IEEE
   10.you tube RSA algorithm in B..Hariharan