A Hybrid Cryptography Algorithm for Cloud Computing Security

Divya Prathana Timothy[1]
SITE
Vellore Institute of Technology
Vellore (T. N), India
divyaprathana.timothy@vit.ac.in

Ajit Kumar Santra[2]
SITE
Vellore Institute of Technology
Vellore (T. N), India
ajitkumar@vit.ac.in

Abstract— **In the present scenario, the Cloud Computing is very famous and flexible technology. It facilitates customers with effortlessness, quickness, competence etc in their work area through the services. Cloud provides huge data centre to handle the large amount of information. The Cloud Computing benefits the organizations to handle their large volume of information. The main issue in cloud computing is data security, because number of customers are sharing same cloud. This study aimed at designing a new security method by using a hybrid cryptosystem, for data security in the cloud. The need for the current investigation is to protect data from unauthorized access or hackers in cloud at the time of data transmission by encrypting the user data. Cloud computing constitutes several security issues including data access control, identity management, auditing ,integrity control and risk management therefore, this hybrid cryptosystem is designed and comprises of both symmetric and asymmetric cryptography algorithm in which Blowfish symmetric algorithm deals with data confidentiality whereas, RSA asymmetric algorithm deals with an authentication. This method also includes the Secure Hash Algorithm – 2 for data integrity. The present study concluded that the proposed method provides high security on data transmission over the internet and proper network access on demand to a shared tank of constructive computing resources, mainly net, server, and storage application.**

Keywords—blowfish; cloud-computing; cryptosystem; RSA; SHA-2.

I. INTRODUCTION (*HEADING 1*)

The Cloud Computing is a powerful technology which is used to manage information's and applications on-demand. Cloud computing is reliable and consistent, due to this organization do not need to build or maintain their own in-house computer Infrastructure. It provides resources like Software, Applications and Services to their Customers. Cloud computing is cost saving technology for any type or size of business and organization, just like electricity bill they have to pay for cloud computing resources based on their consumption. Cloud computing is famous for allowing proper network access on demand to a shared tank of constructive computing resources, mainly net, server, and storage application. That can be quickly provisioned and discharged with negligible administration or service supplier. Today, most of the businessmen's, application developers, officers and students are using cloud on a regular basis because it is easily accessible. Cloud is profitable because of its characteristics like On-Demand administration, Resource pooling, Broad net access, Rapid flexibility and the most important one is Measured service in which user has to pay for services according to their service usage (just like electricity bill).

Though cloud has many advantages, it has some disadvantages as well, and one of them is security issue. Cloud computing has a number of security issues such as data access control, identity management, risk management, auditing and logging, integrity control, infrastructure and dependent risks. If any organization is using cloud computing, they should provide their important data to service provider. The possibility of sensitive information going to wrong hand is increasing due to cloud services being easily accessible and available for all. The organizations cannot take risks with their sensitive information. Hence, there is a need to resolve the security issue of cloud computing.

Secure data transmissions prevent contact lists and personal e-mail from being read by someone other than the intended recipient, keep firmware upgrades out of devices they don't belong in, and verify that the sender of a piece of information is who he says he is. The sensibility of data security is even mandated by law in certain applications: in the U.S. electronic devices cannot exchange personal medical data without encrypting it first, and electronic engine controllers must not permit tampering with the data tables used to control engine emissions and performance.

To solve the data security and privacy issue in cloud computing number of methodology is introduced. There are many risk management is defined. Different ideas or solutions are applied in cloud computing. One of the solutions for data security and integrity problem is encryption.

Jain and Agrawal [1], have proposed a hybrid cryptography algorithm using a combination of two symmetric cryptographic technique, viz Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) to strengthen the encryption algorithm. Authors are mainly concerned about the security of sensitive data transfer over different networks for example Military data and Banking transactions etc.

Sheikh and kaul [2], introduced a hybrid model using a combination of encryption algorithms well known as Advanced Encryption Standard (AES) and Blowfish for Data Confidentiality, Message Digest-5 (MD-5) for Data integrity, Elliptic Curve Diffie Hellmann Algorithm (ECDHA) for Key

978-1-5386-1716-8/17/$31.00 ©2017 IEEE

exchange, and Elliptic Curve Digital Signature Algorithm (ECDSA) for Digital signature. They also evaluated the Performance of Encryption algorithms based on throughput, and time of encryption/decryption.

Ali [3], defined a hybrid encryption algorithm using Advanced Encryption Standard (AES) and Blowfish encryption algorithm for specific application like in bank, military, big websites those handle big data base, and in network companies etc. Author also examined different encryption algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish Encryption algorithm and Rivest Shamir Adleman (RSA) Encryption algorithm with the help of Statistical Tests.

El_etriby et al. [4], have focused on the security of data storage in the desktop and cloud. They have presented a comparison of the eight encryption algorithms such as: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), Rivest Cipher 4 (RC4) Encryption, Rivest Cipher (RC6) Encryption, Two-Fish Encryption, Blow-Fish Encryption, and MARS Encryption at desktop computer and at Amazon Elastic Compute Cloud (Amazon EC2) cloud computing environment. The algorithms are assessed by arbitrariness testing by utilizing NIST factual test as a part of cloud environment. Pseudo Random Number Generator (PRNG) is utilized to finish up the most suitable technique.

Najar and Dar [5], have proposed efficient, tough and secure hybrid encryption algorithm design with the help of Symmetric key algorithm like Advanced Encryption Standard (AES) and Asymmetric key algorithm like Rivest Shamir Adleman (RSA) algorithm which is responsible for management of key, and Secure Hash Algorithm-1 (SHA-1) used for digital signature.

Shereek et al. [6], provided a method by using the Rivest Shamir Adleman (RSA) algorithm and Fermat's theorem to build a secure environment for cloud computing. Authors are also explained that selection of big size number of key in RSA provide the strong cryptosystem but it increases the time of key generation and affect the performance of RSA algorithm. Fermat's little theorem helps to increase the speed of RSA algorithm and improved its performance.

Rao and Padmanabham [7], defined a new security scheme for integrity, authentication and confidentiality of files which are stored on the cloud. Message Digest -5 (MD5) algorithm is used for achieving data integrity, Blowfish algorithm is used for data confidentiality, and Rivest Shamir Adleman (RSA) algorithm for authentication.

Sengupta [8], proposed a hybrid Rivest Shamir Adleman (RSA) algorithm to provide high data security in the cloud. Author also conclude that single RSA algorithm is not sufficient to secure data on the cloud therefore Feistel Encryption Algorithm is used after RSA encryption algorithm to reduce the chances of man-in-the-middle attack.

Thakur and kumar [9], demonstrated that blowfish encryption algorithm is better than other Symmetric key cryptography algorithms such as DES and AES. They analyzed the performance of DES, AES and Blowfish Encryption algorithm on the basis of different parameters such as block size, key size and speed.

Suresh and Prasad [10], described about the Cloud Computing security problems, attacks and some security algorithms such as Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), and Message Digest -5 (MD-5).

Seth et al. [11], is about providing security for the data that is to be transferred over internet so that any intruder should not change the data before the intended receiver receives it. This paper proposed a new methodology in which Token-id is generated automatically for individual service of cloud. Authors are provided more reliable, worthwhile and safe environment for cloud computing using auto generated Token-id with Digital signature. The use of above mentioned technique can reduce the security threats so that the confidentiality of data is achieved.

This paper proposed a new hybrid cryptography method to solve the data security and privacy issues of cloud computing. The aim is to achieve safe transmission of confidential information by applying hybrid encryption algorithm which is a combination of Blowfish symmetric and RSA asymmetric cryptographic algorithm, and also digital signature on transmitting data.

II. METHODOLOGY

This new hybrid cryptography method includes the combination of both symmetric and asymmetric algorithm for more excellent result. Each cryptography method follows the encryption and decryption process. In encryption process the original data is transformed into cipher data, which is not understand by any human or person. To get the original data from cipher data decryption process is used. In this study two time encryption and decryption process is performed because the use of symmetric and asymmetric algorithm.

A. Encryption

Encryption process converts the original data into cipher data with the help of Blowfish algorithm. Blowfish algorithm is a symmetric key cryptography method, which uses secret key to encrypt the original data and send this key with encrypted data to the receiver. The risk involved in symmetric cryptography is the shifting of secret key over the internet. To overcome the risk of symmetric cryptography, RSA algorithm is used which is an asymmetric key cryptography method.

Blowfish algorithm is responsible for encryption of data, which is selected by the user. Blowfish is a symmetric cryptographic algorithm which uses single key to encrypt and decrypt the original data. This single key is known as secret key. Secret key is transmitted with encrypted data over the internet and hence need to encrypt the secret key. This secret key is encrypted using RSA algorithm, which is an asymmetric cryptographic algorithm. RSA algorithm uses different key for encryption and decryption.

Signature generation phase provides the message authentication with the help of Digital signature using SHA-2. For secure transmission and authorization, digital

signature is used. Digital signature assures that the data is authorized by authenticated person; it is not modified by any third person during data transmission. Private key is used for digital signature on message digest. Message digest is produced by applying Secure Hash Algorithm-2 (SHA-2) on encrypted user data.

SHA-2 is a message digest function with a block size of 512- bit generates 256-bit message digest.

TABLE I Comparison between MD 5 and SHA [12]

Sr. No.	Comparison Parameters	MD-5	SHA
1	Security	Less Secure	High Secure
2	Message Digest Length	128 bits	160 bits
3	Attack required to find out original message	2^{128} bit operation	2^{160} bit operation
4	Attacks to try and find two messages producing the same MD	2^{64} bit operation	2^{80} bit operation
5	Speed	Faster, only 64 iteration	Slower, required 80 iteration

TABLE II Comparison of SHA Functions

Sr. No.	Algorithm and Variant	SHA 0	SHA 1	SHA 2	
1	Output size	160 bits		256/224 bits	512/384 bits
2	Internal state size	160 bits		256 bits	512 bits
3	Block size	512 bits		512 bits	1024 bits
4	Max message size	2^{64} -1 bits		2^{64}-1bits	2^{128}-1bits
5	Word size	32 bits		32 bits	64 bits
6	Rounds	80		64	80
7	Operations	AND, OR, XOR, shr, ROT, ADD (2^{32})		AND, OR, XOR, shr, ROT, ADD (2^{32})	AND, OR, XOR, shr, ROT, ADD (2^{64})
8	Security bits	<34 (Collision found)	<63 (Collision found)	112 128	192 256 112 128

Table 1 and table 2, shows why SHA 2 is better than other hash algorithms such as MD 5 and SHA-1.

B. Decryption

In decryption process cipher data is converted into original data. In this cryptography method first phase is hybrid decryption phase and second phase is signature verification phase. Hybrid decryption phase is a reverse process of hybrid encryption phase. This phase is responsible for decryption of encrypted message with the help of RSA and Blowfish. First step, RSA decryption algorithm decrypts the encrypted key, which helps to get original data. Second step, with the help of decrypted key blowfish decryption algorithm decrypt the encrypted data.

In signature verification phase, message digest is generated using SHA 2 to verify the signature.

III. PROPOSED ALGORITHM

A. Encryption Process

Basic function of this project is to encrypt the user data to protect data from unauthorized access or hackers in cloud at the time of data transmission also. After encryption data will convert into cipher text.

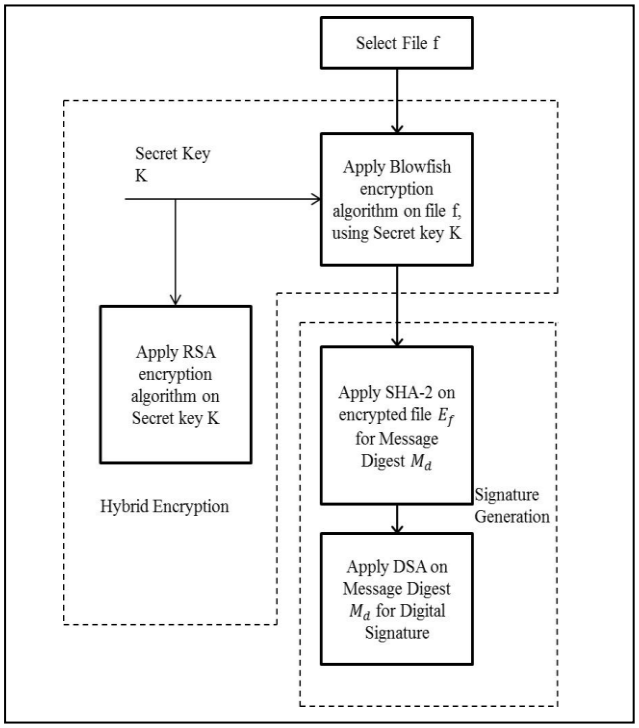


Figure1: Encryption Process

(i) Select a secret key K between the ranges of 448 bits to 1024 bits of variable length.

(ii) Encrypt the selected file f, by applying Blowfish algorithm with the help of secret key. Blowfish algorithm is a symmetric key cryptographic algorithm, which uses single key to convert the original data into cipher data and vice versa. This key is known as secret key or private key. It has a 64 bit block size and the length of key is from 32 bits to 448 bits.

$$E_f = EB_K(f)$$

(iii) Encrypt the secret key K, using RSA algorithm. RSA algorithm is an Asymmetric key cryptographic algorithm, which uses pair of key for encryption and decryption.

$$E_K = ER(K)$$

(iv) Apply SHA 2 on encrypted file E_f to generate message digest or hash code. SHA stands for Secure Hash Algorithm, which is used to generate the message digest.

$$M_d = S(E_f)$$

(v) Apply digital signature algorithm on message digest to generate digital signature.

$$D_s = D(M_d)$$

B. Decryption Process

Decryption process converts the cipher text into original data, so that user can read or access this data. Only authorized user can decrypt the cipher text or in other word only authorized user can access the data.

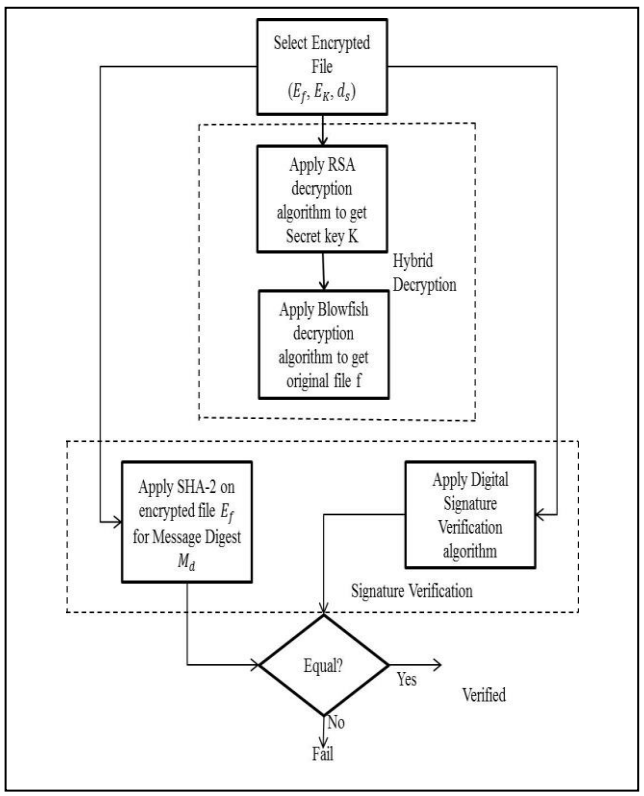


Figure 2: Decryption Process

(i) To get the secret key K, decrypt the encrypted secret key E_K by applying RSA decryption algorithm.

$$K = DR(E_K)$$

(ii) Using above secret key, obtain the original file f, by applying blowfish decryption algorithm on encrypted file E_f.

$$f = DB_K(E_f)$$

(iii) Apply verification algorithm of digital signature on digital signature on d_s to get the expected message digest or hash code.

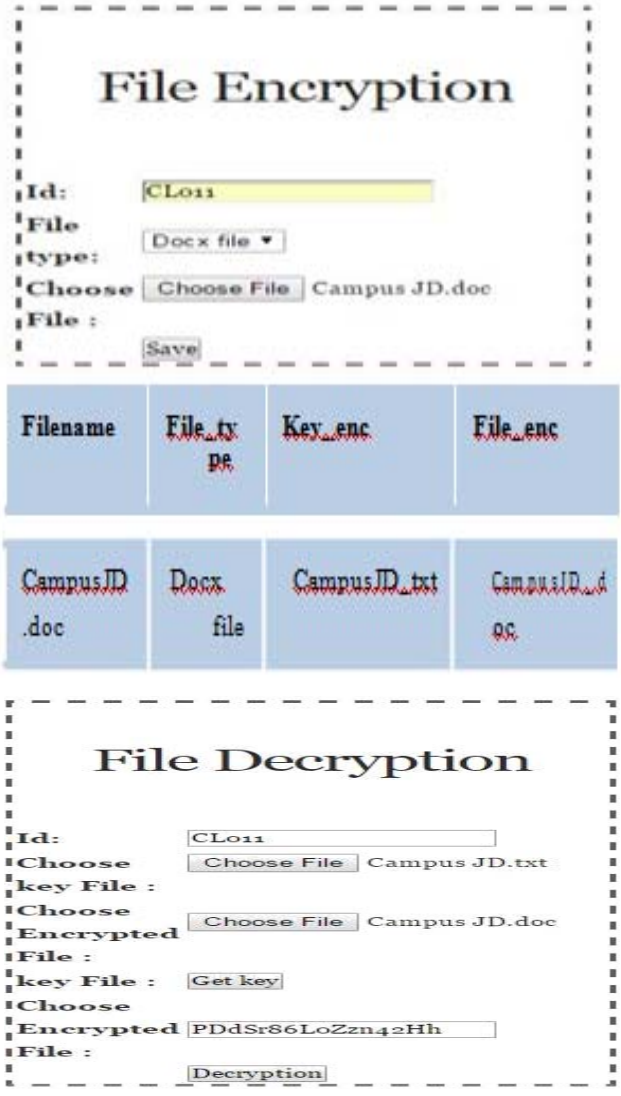
$$M_d = V(Ds)$$

(iv) Compare this message digest or hash code with the SHA 2 generated message digest or hash code.

$$M_d = S(E_f)$$

IV. RESULT AND DISSCUSSION

The proposed method protected the user data, from unauthorized access at the time of transmission and also in Amazon Simple Storage Service Bucket. Proposed system increased the difficulty level for unauthorized person or hacker to decrypt the encrypted data, through encrypted key, via RSA.



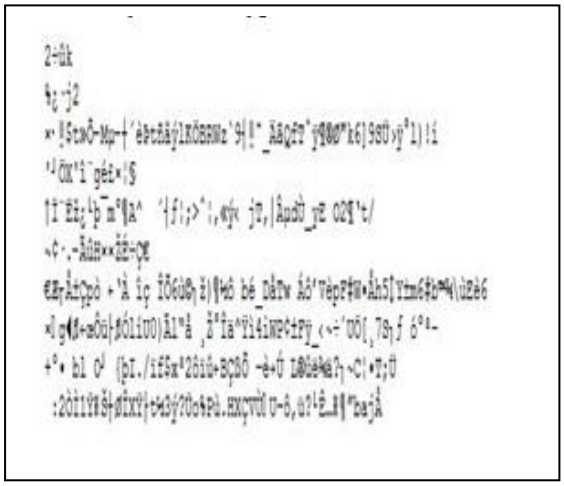
Input File: CampusJD.doc

Selection Process:

- Group Discussion / Extempore
- Communication Assessment
- Technical Assessment
- Please Inform candidates to carry 1PassPort Size Photo and a resume copy

Sample document created with MS Word
Page 1 of 5
This page is Size Letter
0
1
2 If this was a real document it would have more here.
3
4 Sample: Times New Roman

After Hybrid Encryption



V. CONCLUSION

A new hybrid cryptography algorithm is proposed using Blowfish, RSA, and SHA-2 algorithms. The combination of symmetric and asymmetric algorithm provides efficiency to proposed system. The proposed method provides high security on data transmission over the internet using SHA-2 algorithm.

REFERENCES

[1] Mahavir Jain, and Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", International journal of Core Engineering & Management, Volume 1, Issue 3, pp. 1-8, June 2014.

[2] P Shaikh, and V. Kaul, "Enhanced Security Algorithm using Hybrid Encryption and ECC", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3, pp. 80-85, May-June 2014.

[3] Ali E.Taki El_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, pp. 669-673, December-2013.

[4] Sherif El-etriby, Hatem S. Abdul-kader, and Eman M. Mohamed, "Modern Encryption Techniques for Cloud Computing", ICCIT, pp. 800-805, 2012.

[5] Jan Mohammad Najar, and Shahid Bashir Dar, "A New Design of a Hybrid Encryption Algorithm", International Journal of Engineering and Computer Science, Volume 3, Issue 11, pp. 9169-9171, November 2014.

[6] Balkees Mohamed Shereek, Zaiton Muda, and Sharifah Yasin "Improve cloud computing security using RSA encryption with Fermat's little theorem", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 4, Issue 2, pp. 1-8, February-2014.

[7] Hanumantha Rao.Galli and Dr.P.Padmanabham, **"** Data Security in Cloud using Hybrid Encryption and Decryption**",** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, pp. 494-497, October-2013.

[8] Dr. Nandita Sengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, pp. 4146-4152, May-2015.

[9] Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol. 1. Issue 2, pp. 06-12, December-2011.

[10] K. S. Suresh and Prof K. V. Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, pp. 110-114, October-2012.

[11] R. K. Seth, Rimmy Chuchra and Simran, "TBDS – A New Data Security Algorithm in Cloud Computing", International Journal of Computer Science and Information Technology, Vol. 5, Issue 3, pp. 2703-2706, 2014.

[12] Piyush Gupta and Sandeep Kumar, "A Comparative Analysis of SHA and MD 5 Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5, Issue 3, pp. 4492-4495, 2014.