CLOUD DATA SECURITY: DEVELOPING AN INNOVATIVE MODEL TO EFFICACIOUSLY USE CROSSBREED CRYPTOSYSTEM IN SAFE GUARDING DATA SECURITY

Adarsh Dhiman

Delhi Public School, Ambala

ABSTRACT

In the present situation, Cloud Computing is essential and adaptable innovation. It encourages clients with ease, snappiness, ability and so on in their work zone through the administrations. Cloud gives a massive server farm to deal with the comprehensive measure of data. The Cloud Computing benefits the associations to deal with their vast volume of data. The primary issue in distributed computing is information security since many clients are sharing the same cloud. This investigation went for structuring another security technique by utilising a crossbreed cryptosystem, for information security in the cloud. The requirement for the present examination is to shield information from unapproved access or programmers in the shadow at the season of information transmission by encoding the client information. Distributed computing establishes a few security issues including information get to control, character administration, evaluating, honesty control and hazard administration along these lines, this crossbreed cryptosystem is planned and contains both symmetric and Hilter kilter cryptography calculations in which Blowfish symmetric calculation manages information secrecy while RSA lopsided calculation manages a confirmation. This strategy additionally incorporates the Secure Hash Algorithm – 2 for information uprightness. The present investigation reasoned that the proposed technique gave high security on information transmission over the web and authorised system access on interest to a mutual tank of productive figuring assets, essentially net, server, and capacity application.

1. BACKGROUND

Cloud Computing is an incredible innovation which is utilised to deal with data's and applications on-request. Distributed computing is dependable and predictable, because of this association do not have to fabricate or keep up their very own in-house PC Infrastructure. It gives assets like Software, Applications, and Services to their Customers. Distributed computing is cost sparing innovation for any sort or size of business and association, much the same as power charge they need to pay for distributed computing assets dependent on their utilisation. Distributed computing is celebrated for permitting legitimate system access on interest to a mutual tank of valuable registering assets, predominantly net, server, and capacity application. That can be immediately provisioned and released with an immaterial organisation or administration provider. Today, a large portion of the businessmen's, application engineers, officers, and understudies are utilising cloud all the time since it is effortlessly open. Cloud is beneficial as a result of its attributes like On-Demand organisation, Resource pooling, Broad net access, Rapid adaptability and the most imperative one is a Measured administration in which client needs to pay for administrations as per their administration utilisation (just like power bill).

Although the cloud has numerous focal points, it has a few hindrances also, and one of them is a security issue. Distributed computing has various security issues, for example, information gets to control, personality administration, hazard administration, examining and logging, trustworthiness control, framework and ward dangers. On the off chance that any association is utilising distributed computing, they ought to give their valuable information to the specialist organisation. The likelihood of touchy data going to the wrong hand is expanding because of cloud administrations being effectively open and accessible for all. The associations cannot go out on a limb with their delicate data. Subsequently, there is a need to determine the security issue of distributed computing.

Secure information transmissions forestall contact records and individual email from being perused by somebody other than the planned beneficiary, keep firmware overhauls out of gadgets they do not have a place in, and check that the sender of a snippet of data is whom he says he is. The sensibility of information security is even commanded by law in specific applications: in the U.S. electronic gadgets cannot trade individual therapeutic information without encoding it first, and electric motor controllers must not allow messing with the information tables used to control motor outflows and execution.

To fathom the information security and protection issue in distributed computing number of the procedure is presented. There are many hazard administration is characterised. Distinctive thoughts or arrangements are connected in distributed computing. One of the answers to information security and trustworthiness issue is encryption.

Jain and Agrawal [1], have proposed a mixture cryptography calculation utilising a blend of two symmetric cryptographic methods, viz Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) to fortify the encryption calculation. Creators are for the most part worried about the security of delicate information exchange over various systems for instance Military information and Banking exchanges and so forth.

Sheik and Kaul [2], presented a half and half model utilizing a blend of encryption calculations surely understood as Advanced Encryption Standard (AES) and Blowfish for Data Confidentiality, Message Digest-5 (MD-5) for Data uprightness, Elliptic Curve Diffie Hellmann Algorithm (ECDHA) for Key trade, and Elliptic Curve Digital Signature Algorithm (ECDSA) for Digital mark. They additionally assessed the Performance of Encryption calculations dependent on throughput, and time of encryption/decoding.

Ali [3], characterised a half and half encryption calculation is utilising Advanced Encryption Standard (AES), and Blowfish encryption calculation for a particular application like in a bank,

military, large sites those handle huge information base, and in system organisations and so on. Creator likewise analysed different encryption calculations like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish Encryption calculation and Rivest Shamir Adleman (RSA) Encryption calculation with the assistance of Statistical Tests.

El_etriby et al. [4], have concentrated on the security of information stockpiling in the work area and cloud. They have introduced a correlation of the eight encryption calculations, for example, 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 personal computer and at Amazon Elastic Compute Cloud (Amazon EC2) distributed computing condition. The calculations are surveyed by assertion testing by using NIST real test as a piece of cloud condition. Pseudo Random Number Generator (PRNG) is used to complete the most appropriate method.Najar and Dar [5], have proposed efficient, sturdy and secure hybrid encryption algorithm design with the help of Symmetric key algorithms 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 significant size number of key in RSA provides the strong cryptosystem, but it increases the time of key generation and affects the performance of RSA algorithm. Fermat's little theorem helps to increase the speed of the 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, the 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. The author also concludes that a single RSA algorithm is not sufficient to secure data on the cloud. Therefore, Feistel Encryption Algorithm is used after the RSA encryption algorithm to reduce the chances of a man-in-the-middle attack.

Thakur and Kumar [9], demonstrated that the blowfish encryption algorithm is better than other Crucial symmetric cryptography algorithms such as DES and AES. They analysed the performance of DES, AES and BlowfishEncryption algorithm from different parameters such as block size, key size and speed.

Suresh and Prasad [10], described 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 the 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 has generated automatically for individual service of the cloud. Authors are provided with amore reliable, worthwhile and safe environment for cloud computing using auto-generated Token-id with Digital signature. The use of the above-mentioned technique can reduce 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 a hybrid encryption algorithm which is a combination of Blowfish symmetric and RSA asymmetric cryptographic algorithm, and also the digital signature on transmitting data.

II. METHODOLOGY

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

A. Encryption

Encryption process converts the original data into cypher data with the help of the Blowfish algorithm. Blowfish algorithm is a symmetric key cryptography method, which uses a 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 the secret key over the internet. To overcome the threat of symmetric cryptography, the RSA algorithm is used which is an essential asymmetric cryptography method.

Blowfish algorithm is responsible for encryption of data, which is selected by the user. Blowfish is a symmetric cryptographic algorithm which uses a single key to encrypt and decrypt the original data. This unique key is known as a secret key. The secret key is transmitted with encrypted data over the internet and hence need to encrypt the secret key. This secret key is encrypted using the RSA algorithm, which is an asymmetric cryptographic algorithm. RSA algorithm uses a 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 andauthorisation, the digital name is used. A digital signature assures that the data is authorised by the authenticated person; it is not modified by any third person during data transmission. The private key is used for a digital signature on message digest. The 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 a 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 the decryptionprocess,cypher data is converted into original data. In this cryptography method,the first phase is a hybrid decryption phase and the second phase isthe 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. The first step, RSA decryption algorithm decrypts the encrypted key, which helps to get original data. The second step, with the help ofdecrypted key blowfish decryption algorithm, decrypt the encoded data.

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

III. PROPOSED ALGORITHM

A. Encryption Process

The primary function of this project is to encrypt the user data to protect data from unauthorised access or hackers in the cloud at the time of data transmission also. After encryption data will convert into ciphertext.

(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 the Blowfish algorithm with the help of a secret key. Blowfish algorithm is a symmetric key cryptographic algorithm, which uses a single key to convert the original data into cypher data and vice versa. This key is known as a secret key or a private key. It has a 64-bit block size, and the length of the core is from 32 bits to 448 bits.

Ef = EBK(f)

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

EK = ER(K)

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

Md = S(Ef)

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

Ds = D(Md)

B. Decryption Process

Decryption process converts the ciphertext into original data so that user can read or access this data. The only authorised user can decrypt the ciphertext or in another word only authorised user can access the data.

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

K= DR(EK)

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

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

Md = V(Ds).

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

Md = S(Ef)

IV. FUTURE PROSPECTS

The proposed method protected the user data, from unauthorised access at the time of transmission and also in Amazon Simple Storage Service Bucket. Proposed system increased the difficulty level for an unauthorised person or hacker to decrypt the encrypted data, through the encrypted key, via RSA.A new hybrid cryptography algorithm is proposed using Blowfish, RSA, and SHA-2 algorithms. The combination of symmetric and asymmetric algorithm provides efficiency to the proposed system. The proposed method offershigh security on data transmission over the internet using anSHA-2 algorithm.