ENHANCING THE DATA SECURITY IN CLOUD USING HYBRID ALGORITHM

1Ponnuru Sowjanya, 2K. V. N. Sunitha,
1Research Scholar, JNTUH, Hyderabad,
sowjanya.ponnuru@gmail.com
2BVRIT Hyderabad College
of Engineering for Women, Hyderabad,
k.v.n.sunitha@gmail.com

June 13, 2018

Abstract

Cloud computing is an era in today’s world. It is the latest effort in offering and managing computing as a service. The user in this service can store, manage and access data as per his requirements with reasonable cost. So, maintaining the security of data for this service plays a major role. This data security can be achieved through some encryption algorithms.

The objective of this paper is to discuss measures to enhance the data security by combining the two algorithms to form a hybrid algorithm. Several security issues possible on cloud are further discussed. In this proposed work, we combine the RSA and Blowfish algorithms to form a hybrid algorithm.

Keywords: Cloud computing, Encryption, RSA, Blowfish, hybrid algorithm.
1 Introduction

Cloud computing is a new trend in the development of technologies. Cloud storage enables many users to work together and it allows the user to share the data and the resources [3]. Cloud service provider will provide the data, resources, equipment, and storage space to the users. Users can quickly get resources with low prices. Cloud computing follows ‘pay as you go’ service. The main aim of cloud storage is to provide security of data to the users. This security mainly depends on the terms of authentication, integrity, confidentiality and availability of data.

Authentication: It is a process of confirming whether the user is genuine or authorized to access the data.

Confidentiality: It determines the level of privacy to the data provided by the service provider.

Integrity: This term explains about the trustworthiness of data in the cloud.

Availability: The data must be available at any point of time.

While maintaining all these issues there is a chance of missing security measures. The possible security issues raised in maintaining security are described below [1], [4].

Security issues in Cloud:

1. Secure Data Transfer: In cloud, the storing of data and the physical location of the user is different. So the data transfer should be done in a secured manner.

2. Secure Channel: Here we have to check to what extent the channel is trustworthy.

3. Division of Data: The accessing rights of the individual user and the service provider are different. So, we divide the personal data and remaining data by following some accessing measures [4].

4. User Access Control: Access control mainly prohibits or limits the users from accessing the data.

So, to maintain data security we follow the data encryption or security algorithms before transferring the data from sender to receiver.
Classification of security algorithms: Security algorithms can be classified as symmetric key encryption and asymmetric key encryption [2].

Symmetric key Encryption: In symmetric key encryption, we will use only one key for both encryption and decryption. Here the sender and receiver use the same key [5].

This symmetric encryption is low cost with high speed but provides less security. So, there may be chance of malicious attacks during the transformation of data.

Eg: Blowfish.

Asymmetric key Encryption: Asymmetric key encryption uses two keys. One key is for encryption (public), another key is for decryption (private) [5]. It is slow in speed and also expensive but it is more secure when compared with symmetric key encryption.

Eg: RSA, Diffie Hellman.
2 Existing System

Some of the existing algorithms available to provide the security are discussed further.

a. RSA
b. Diffie Hellman
c. Blow fish

**a. RSA:** It is an asymmetric encryption which uses two keys, i.e. public and private. For example, if the service provider wants to send data to some user then the provider first encrypts the data and then transmitted to end user with public key and the end user decrypts the data with the private key [6].

**How the public key and private key generated:**
RSA algorithm is mainly dependent on the prime numbers and the algorithm [7] is

a. Choose two different prime numbers.
b. Calculate modulus i.e. \( n = pq \).
c. Totient function \( \phi(n) = (p-1)(q-1) \).
d. Choose an integer 'e' i.e. \( 1 < e < \phi(n) / \gcd(e, \phi(n)) = 1 \). e.
   Calculate \( d = 1 + k \cdot \phi(n)/e \).

Encryption \( C = M^e \mod n \).
Decryption \( M = C^d \mod n \).

**b. Diffie Hellman key exchange:** Two keys are used to provide the inter communication between the sender and the
receiver. Another key is used to exchange the data. Here the sender and receiver do not know each other. So there may be a chance of man in the middle attack [8].

A disadvantage of using symmetric key cryptography for encryption is speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method.

**c. Blowfish:** It comes under symmetric algorithm whose key length is longer when compared to remaining symmetric key algorithms. It uses the 64 bit length key for encryption and decryption [9].

It consists of two parts.

**Sub key generation:**
The 64 bit key is divided into two 32 bits (left 32, right 32).
The left 32 bits are XORed with the first element in the p-array to create a value call it as p1 then this p1 is run through a transmission function called f. Then XOR with right 32 bits to produce a new value call it as f1.

**Encryption and Decryption:**
F1 replaces the left half of the message and p1 replaces the right half of the message and the process is repeated 15 more times with successive members. The resulting p1 and f1 is XORed with the last two elements in the p-array to produce the cipher text. Decryption is similar to encryption, with the reversal of p-array values [10].

The main limitation of the Blowfish algorithm is, it must generate a key to the user out of band and especially not through the unsecured transmission channel. All the users need a unique key as, with the number of users increase, management of key generation becomes complicated.

**Hybrid RSA Encryption Algorithm:**
In this algorithm first will apply RSA Encryption algorithm and then will apply Feistel Encryption algorithm to create a cipher text. In the same way will decrypt the cipher text into a plain text. By this hybrid algorithm will control the man in the middle attack [12].

So, to improve the security level, the proposed frame work is going to combine the RSA Encryption algorithm with the blowfish algorithm whose key length larger when compared with the...
remaining algorithms.

3 Proposed System

Here to increase the level of security, an algorithm is developed by combining one symmetric key encryption algorithm and one asymmetric key encryption algorithm to form hybrid algorithm[11].

The main goal of service provider is to generate a cipher text that makes harder to decrypt into plain text. This is possible when the length of the key is longer. So, blow fish algorithm whose length is longer in symmetric key encryption is combined with the RSA in asymmetric key encryption which forms hybrid encryption algorithm.

Steps:

Here first the plain text p is encrypted with RSA Encryption algorithm which produces an encrypted text p1.

Next p1 is again encrypted with the Blowfish Encryption algorithm which produces the cipher text. The encryption process has shown in the below structure.
For decryption first the RSA algorithm is decrypted. The Blowfish Decryption is applied and finally it returns the plain text to the end user. The decryption process has shown in the below structure.

**Blowfish algorithm:** This algorithm is under the classification of a symmetric key cryptographic algorithm.

**Operations:**
Subkey Generation Data Encryption

**Subkey Generation:**
1. key size is from 32-448 bits.
k1, k2, k3, ..........kn where 1 ≤ n ≤ 14
2. p-array, consisting of 18-32 bit subkeys. p1, p2, p3, ..........p18 this p-array is based on the digits of pi. convert this digits of pi into hexa decimal.
3. 4 s-boxes, each box contains 256 4-byte entries.
s1,0,s1,1,.........s1,255
s2,0,s2,1,.........s2,255
s3,0,s3,1,.........s3,255
s4,0,s4,1,.........s4,255

**Data Encryption:** It has a function to iterate 16 times of network. Each round consists of a key, data-dependent substitution and a key-dependent permutation. All operations are XORs and additions on 4-byte words.
Divide w into two 4-byte halves: wL, wR
For \( j = 1 \) - 16:
\[
\begin{align*}
\text{wL} &= \text{wL} \text{ XOR } P_j \\
\text{wR} &= F(\text{wL}) \text{ XOR } \text{wR} \\
\text{INTERCHANGE } &\text{wL and wR} \\
\text{INTERCHANGE } &\text{wL and wR} \\
\text{wR} &= \text{wR} \text{ XOR } P_{17} \\
\text{wL} &= \text{wL} \text{ XOR } P_{18} \\
\text{Recombine } &\text{wL and wR}.
\end{align*}
\]

RSA Algorithm:
Key Generation Algorithm
1. select two large random prime numbers \( x \) and \( y \).
2. Calculate \( m \) and \( \phi(m) \): \( m = xy \) and \( \phi(m) = (x-1)(y-1) \)
3. select a number \( n \), where \( 1 \leq n \leq \phi(m) \) such that:
   \[ \gcd(n, \phi(m)) = 1 \] (where \( \gcd \) means greatest common denominator)
4. Calculate \( p \), where \( 1 < p < \phi(m) \) such that:
   \[ np \equiv 1 \pmod{\phi(m)} \]
the public key is \( (m, n) \) and the private key is \( (m, p) \)
the values of \( x, y \) and \( \phi(m) \) are private
\( n \) is the public or encryption exponent \( p \) is the private or decryption exponent

Encryption: The plain text is converted by the formula \( C = Mn \mod m \) where \( M \) is the original message.
Decryption: The original message \( M \) can be found from the ciphertext \( C \) by the formula \( M = Cp \mod m \).

4 Experimental Study

The experimental study is aimed to compare the results of hybrid algorithm to achieve the high level of security on cloud storage. The level of security has compared based on the parameters key length and the time. By using these parameters the proposed algorithm uses less time and key length when compared with the remaining hybrid algorithms.

The Performance analysis: The proposed model BLOWFISH+RSA and other contemporary models RSA+AES, AES+DES, and TWOFISH+BLOWFISH has been considered for performance analysis to achieve high level of security in cloud data storage. The proposed model outperformed...
the other 3 hybrid models in regard to the key length and time, which are shown in the below table and the graph.

Table 1: Comparison of Length and Time with Different Hybrid Algorithms

<table>
<thead>
<tr>
<th>Hybrid algorithms</th>
<th>Key length</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blowfish+RSA</td>
<td>150</td>
<td>14</td>
</tr>
<tr>
<td>RSA+AES</td>
<td>214</td>
<td>21</td>
</tr>
<tr>
<td>AES+MD5</td>
<td>160</td>
<td>18</td>
</tr>
<tr>
<td>Twofish+Blowfish</td>
<td>192</td>
<td>18</td>
</tr>
</tbody>
</table>

By seeing the results, it is observed that to achieve the level of security by all the hybrid models the BLOWFISH+RSA has taken the less time and key length.

Figure 4: Level of security observed based on the key length and Time

By seeing the results, it is observed that to achieve the level of security by all the hybrid models the BLOWFISH+RSA has taken the less time and key length.
5 Conclusion

The proposed algorithm focuses on providing security to the data in the cloud. The protection of data has to be maintained at the service provider side, data transmission channel also at the end user side. This can be achieved through the proposed algorithm. The results of proposed model BLOWFISH + RSA and other contemporary models RSA + AES, AES + DES, and TWOFISH + BLOWFISH are compared. The performance analysis evincing that the proposed model has outperformed the other contemporary models to achieve the data protection on cloud.

References


