A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing

R.Gowthami Saranya¹, A.Kousalya²

¹Student, Computer Science and Engineering, United Institute Of Technology, Tamilnadu, India
²Assistant Professor, Computer Science and Engineering, United Institute Of Technology, Tamilnadu, India

Abstract—Cloud computing is a word which is describe different computing concepts which contains hugenumber of computers attached through a real-time communication like internet. Cloud computing is also called distributed computing over the network i.e. the ability to execute an application or a program on many computers at the same time. Cloud Computing is an emerging technology in today’s business era. It allows convenient on demand access to resources that involve large number of computers connected through Internet. Public clouds vendors offer many resources such as application, storage, hardware, software’s etc. The security issues present in public cloud is more challenging. As everything is accessed publically; many users have the threat to store and retrieve it publically. As many organizations are moving data to the cloud there is a need to protect data against unauthorized access. Hence it is necessary to study the security issues in public cloud to secure data. The purpose of this paper is to provide an overview of public cloud computing and the security issues involved. This paper deals with the different algorithms or method used for securing data in public cloud.


I. INTRODUCTION

Encryption is the way of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption. There are various types of data encryptions which form the basis of network security. Encryption schemes are dependent on block or stream ciphers. The length and type of the keys utilized depend on the encryption algorithm and the amount of security needed. Inconventional symmetric encryption a single key is used. The data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by third party users. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are not same. The public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message [1].

II. BENEFITS

- **Cost Consumption** — Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.
- **Management** — Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
- **Flexibility** — Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary.
- **Redundancy** — Services using multiple redundant sites can support business continuity and disaster recovery.
- **User Accessible** — Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

III. CHARACTERISTICS

- Hardware infrastructure architecture was based on the clusters, which was large-scale and low-cost. The infrastructure of cloud computing was composed of a large number of low-cost servers, and even the X86 server architecture. The strong performance, the fundamental mainframe’s prices were also very expensive.
- Collaborative development of the underlying services and the applications is to achieve maximum resource utilization. By this way, application’s construction is improved. But for traditional computing model, applications to be complete dependent on the underlying service.
- The redundant problem among multiple low-cost servers is solved by the software method. Because of using a large number of low-cost servers, Failure between nodes cannot be ignored, so the issue of fault tolerance among nodesshould be taken into account, when designing software [2].
IV. SECURITY ISSUES IN CLOUD COMPUTING

- Transmit and store user’s information as little as possible. After systemic analysis, the cloud computing applications will collect and store the most necessary information only.
- Security measures will be adopted to prevent unauthorized access, copying, using or modifying personal information.
- Achieve user’s control to the greatest degree. Firstly, it is necessary to allow the user to control the most critical and important personal information. Secondly, it is available to manage personal information by a trusted third party.
- Allow users to make choice. Users have the right to select the use of personal information. Besides, they can join or leave freely.
- Make clear and limit the purpose of use of data. Personal information must be used and handled by the person with specific identification for specific purpose and owner of information should be notified before using.
- Establish feedback mechanism to ensure that safety tips and detailed measures of the service will be provided to the user timely.
- It can maximize the security of user’s data after introducing principles above [3].

V. LITERATURE SURVEY

Encryption algorithm play a vital role, to provide secure communication over the network. Encryption is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using “the key” and only user have the key to decrypt the data. To techniques in Security algorithms are Symmetric Algorithms and asymmetric Algorithms.

A. DES

DES stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher [4].

Algorithm:

```
function DES_Encrypt (N, K) where M = (L, R)
    N ← IP(N)
    For round ← 1 to 16 do
        Ki ← SK (K, round)
        L ← L xor F(R, Ki)
    swap(L, R)
    M ← IP−1(N)
end
return N
```

B. BLOWFISH

Blowfish algorithm was developed in 1993. It is one of the most common algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [5].

Algorithm

Divide x into two 32-bit halves: x_L, x_R

For i = 1 to 16:
    X_L = X_L XOR P_i
    X_R = F(X_L) XOR X_R
    Swap X_L and X_R
Next i

Swap X_L and X_R (Undo the last swap.)

x_R = x_R XOR P_{17}
x_L = x_L XOR P_{18}
Recombine x_L and x_R

C. RC2

RC2 is a symmetric block cipher that operates on 64 bit quantities. It uses a variable size key, but 128 bit key would normally be considered good. RC2 can be used in all the modes that DES can be used. A proprietary algorithm developed by RSA Data Security, Inc. The algorithm expands every single message by up to 8 bytes. RC2 is a block cipher that encrypts data in blocks of 64 bits [6].

D. RC5

RC5 was developed in year 1994. The key length if RC5 is MAX2040 bit. The block size of RC5 is 32, 64 or 128. The use of RC5 algorithm shows that it is Secure. The speed is slow [7].
Algorithm
C = C + S[0];
D = D + S[1];
for i = 1 to f do
C = ((C Xor D) <<< D) + S[ 2 * i ]
D = ((D Xor C) <for i = 1 to f do
Next

E. RC6
RC6 algorithm has a block size of 128 bits. The key sizes of 128, 192 and 256 bits. RC6 is developed in same structure of RC5, having data-dependent rotations, XOR operation and modular addition. RC6 could be viewed as interweaving two parallel RC5 encryption Techniques. Though, RC6 can use an extra multiplication operation not present in RC5 in order to make the rotation dependent on each bit, and not the least significant few bits[6].

F. 3DES
3DES was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied three times to increase the encryption level. But 3DES is slower than another block cipher methods. 3DES is an enhancement of DES and it is 64 bit block size and with 192 bits key size. 3DES requires always more time than DES because of its triple phase encryption characteristics. 3DES has lower performance in terms of power consumption and throughput when compared with DES[5][8].

Algorithm
For j = 1 to 3
{ 
C j,[0] = IV j 
For i = 1 to n j
{ 
C j,[i] = E KEY3 (D KEY2 (E KEY1 (P j,i-1 C j,i-1)))
Output C j,[i]
}
}

G. AES
H. AES stands for Advanced Encryption Standard. It is the new encryption standard recommended by NIST to replace DES. The Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. AES have key length of 128, 192, or 256 bits, by default 256. This can encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. AES has been carefully tested for many security applications[8][9].

Algorithm
Cipher(byte[] input, byte[] output)
{
byte [4,4] State;
copy input[] into State[] AddRoundKey for (round = 1; round < Nr-1; ++round)
{
SubByteShiftRowsMixColumnsAddRoundKey
}
SubByteShiftRowsAddRoundKey
copy State[] to output[]
}

I. RSA
RSA was an encryption and authentication technique that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the commonly used encryption techniques. Up-to-Date it is the only algorithm used for private and public key generation and encryption. RSA is a fast encryption[8].

Algorithm
Key Generation: KeyGen(r, s)
Input: Two large primes – r, s
Compute n = r .s
φ(n) = (r - 1)(r - 1)
Choose e such that gcd(e, φ(n)) = 1
Determine d such that e .f ≡ 1 mod φ(n)
Key:
public key = (e, n)
secret key= (f, n)
Encryption:
c = m e mod n
where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product.
Given ci = E(mi) = mi e mod n, then (c1 . c2) mod n = (m1 . m2) e mod n

J. DSA
DSA stands for Digital Signature Algorithm which was proposed by the NIST in August 1991 for use in their DSS and adopted as FIPS 186 in 1993. The four revisions to the initial specification have released. In DSA, the entropy, secrecy, and uniqueness of the random signature value k is critical. DSA is so critical that violating any one of these three requirements can reveal the entire private key to the third party. Using the same value twice, using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA [9].

K. Diffie-Hellman Key Exchange
Diffie-Hellman key exchange was a specific method of exchanging cryptographic keys. The D-H key Exchange is one of the earliest practical examples of key exchange
implemented within the field of cryptography. The D–H key exchange method allows two users that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. In this, the key can then be used to encrypt subsequent communications using a symmetric key cipher[10].

L. TWOFISH

Bruce Schneier is the person who composed Blowfish and its successor Twofish. The Keys used in this algorithm may be up to 256 bits in length. Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Twofish is also freely available to anyone who wants to use it. As a result, we’ll find it bundled in encryption programs such as Photo Encrypt, GPG, and the popular open source software TrueCrypt[11].

M. IDEA

IDEA stands for International Data Encryption Algorithm which was proposed by James Massey and Xuejia Lai in 1991. IDEA is considered as best symmetric key algorithm. It accepts 64 bits plain text. The key size is 128 bits. IDEA consists of 8.5 rounds. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. The basic operations are modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Maximum number of keys used for performing different rounds is 52 [12].

N. ELGAMAL

The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the D–H key exchange. ElGamal was described by Taher Elgamalin 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The DSA is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. The security of ElGamal depends on the difficulty of a particular problem in related to computing discrete logarithms[13].

O. HOMOMORPHIC ENCRYPTION

Homomorphic encryption was a one of encryption technique which allows specific types of computations to be carried out on ciphertext. It gives an encrypted result which when decrypted matches the result of operations performed on the plaintext. When the data is transferred to the cloud we use standard encryption methods to secure this data, but when we want to do the calculations on data located on a remote server, it is necessary that the cloud provider has access to the raw data, and then it will decrypt them [14].

VI. COMPARISON OF EXISTING SECURITY ALGORITHM

In this section, we compare the existing symmetric algorithms on the basis of different parameters as shown in table1, which includes Block Size, Key Length, Security, and Speed.

<table>
<thead>
<tr>
<th>S.NO</th>
<th>CHARACTERISTICS DEVELOPED</th>
<th>BLOCKSIZE (Bits)</th>
<th>KEYLENGTH (Bits)</th>
<th>SECURITY</th>
<th>SPEED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>DES 1997</td>
<td>64</td>
<td>56</td>
<td>Proven Inadequate</td>
<td>Very slow</td>
</tr>
<tr>
<td>2.</td>
<td>BLOWFISH 1993</td>
<td>64</td>
<td>32-448</td>
<td>Considered secure</td>
<td>Fast</td>
</tr>
<tr>
<td>3.</td>
<td>RC2 1987</td>
<td>64</td>
<td>8-128</td>
<td>High secure</td>
<td>Very fast</td>
</tr>
<tr>
<td>4.</td>
<td>RC5 1994</td>
<td>32, 64 or 128</td>
<td>MAX2040</td>
<td>Considered Secure</td>
<td>Slow</td>
</tr>
<tr>
<td>5.</td>
<td>RC6 1998</td>
<td>128</td>
<td>128, 192 or 256</td>
<td>Secure</td>
<td>Fast</td>
</tr>
<tr>
<td>6.</td>
<td>3-DES 1998</td>
<td>64</td>
<td>112, 168</td>
<td>Considered Secure</td>
<td>Slow</td>
</tr>
<tr>
<td>7.</td>
<td>AES 2000</td>
<td>128, 192 or 256</td>
<td>128, 192 or 256</td>
<td>High secure</td>
<td>Very fast</td>
</tr>
<tr>
<td>8.</td>
<td>RSA 1977</td>
<td>128</td>
<td>1024-4096</td>
<td>Considered secure</td>
<td>Very Slow</td>
</tr>
<tr>
<td>9.</td>
<td>DSA 1991</td>
<td>256</td>
<td>192</td>
<td>Secure</td>
<td>Fast</td>
</tr>
<tr>
<td>10.</td>
<td>DIFFIE-HELLMAN 1976</td>
<td>-</td>
<td>-</td>
<td>Not secure</td>
<td>Slow</td>
</tr>
<tr>
<td>11.</td>
<td>TWOFISH 1993</td>
<td>128</td>
<td>128, 192 or 256</td>
<td>Secure</td>
<td>Very Fast</td>
</tr>
<tr>
<td>12.</td>
<td>IDEA 1991</td>
<td>64</td>
<td>128</td>
<td>Inadequate</td>
<td>Slow</td>
</tr>
<tr>
<td>13.</td>
<td>ELGAMAL 1985</td>
<td>-</td>
<td>-</td>
<td>Not secure</td>
<td>Fast</td>
</tr>
<tr>
<td>14.</td>
<td>HOMOMORPHIC ENCRYPTION 1978</td>
<td>-</td>
<td>-</td>
<td>Secure</td>
<td>Fast</td>
</tr>
</tbody>
</table>
VII. CONCLUSION

Data Security has become the most important issue in cloud computing security. Since, Data and Information should not be leaked to the third party user an efficient security algorithms should be implemented. This paper is a survey report on various security algorithms in cloud using cryptographic techniques. Different algorithms use different protection techniques but they all are liable to different situations. So the single security algorithms can’t be trusted. So we conclude that the multilevel security architecture is required for data security for each level in cloud based applications.

VIII. REFERENCES