Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 10, October-2018

Security Analysis of Cryptographic Algorithms in Cloud Computing

U. Thirupalu
Research Scholar
Dept. of Computer Science
S V U CM&CS-Tirupati
India-517502

E. Spandhana
M.Sc Final
Dept. of Computer science
S V U CM&CS-Tirupati
India- 517502

Dr. E. Kesavulu Reddy
Assistant Professor
Dept. of Computer Science
S V U CM&CS-Tirupati
India-517502

Abstract: **Cloud computing is one of the fastest rowing internet based technology. Data encryption is one of the widely used methods to ensure the data confidentiality in cloud environment. In this paper, we discuss the symmetric and Asymmetric algorithms to provide security in the field of cloud computing with different parameters and propose a new approached public key cryptosystem for security in cloud computing.**

Keywords: Security, Encryption, Decryption, Cloud Computing, Data Storage, RSA Algorithm.

I. INTRODUCTION

Cloud computing illustrate Information Technology as a fundamentally diverse operating model that takes advantage of the maturity of web applications and networks and the rising interoperability of computing systems to provide IT services. Data security is becoming a fundamental obstruction in cloud computing. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. Many giant IT firms have launched cloud services viz. Apple, Amazon EC2, Google, Microsoft, Rackspace etc., who provide several storage tier plans
tailored for both consumers and businesses. Some firms may proclaim themselves asloud services, but ironically they tend to serve online backup or file sharing services. Cloud computing combines the data-sharing model and
service statistical model. From a technical point of view, cloud computing has the following three basic characteristics [2]

- Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The
- infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server architecture. Through the strong performance, the traditional mainframe's prices are 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 nodes should be taken into account, when designing software [2].

II. RELATED WORK

In [8] analyze the security challenges in cloud data with overcome the possible solutions. They analyze the different levels of security the data may be process, transmit and depicted. In [9] the issues in security associated with cloud data storage and it is effective to handle certain failures, malicious data modification attack and server colluding attacks. This scheme is drawback to new research areas and leading to unexpected mockeries. In [10] The privacy issues describes in cloud computing and also focuses on the risks, threats, design patterns and accountability with in cloud computing scenario. In this paper [11] provides an overview of security mechanisms in the context of cloud computing and describes various threats and relevance to real-world environment. In this paper [12] they provide the security through public key cryptosystem RSA algorithm and to storage of data in cloud in virtualized environment. The RSA algorithm would guarantee high security, but simultaneously issue is in related to performance.

III. CRYPTOGRAPHIC ALGORITHMS IN CLOUD COMPUTING

They are two types of cryptographic Algorithms are

A. Symmetric key cryptographic Algorithms
B. Asymmetric Key cryptographic Algorithms

A. Symmetric key cryptographic Algorithms

Symmetric key systems use the same key for both encryption and decryption. In order to communicate securely using a symmetric system, two parties must agree on the key using some pre-existing secure channel. When more than two parties are involved key distribution becomes even more complicated, and historically key distribution has been a major obstacle for particle uses of cryptography. Typical symmetric ciphers use very convoluted transformations to obscure any patterns in the original message. The key controls how the transformations operate, and provides a map for reversing a transformations during decryption.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 10, October-2018

- DES
- BLOWFISH
- RC5
- 3DES
- AES

❖ DES

DES is first block symmetric encryption algorithm published by NIST designed by IBM on 1974. The same key is used for both encryption and decryption; DES uses 64-bit key in terms of 8-bits for error correction and 56-bits as a key but in every byte 1 bit in has been selected as a 'parity' bit, and is not used for encryption mechanism. The 56 bit is permuted into 16 sub- keys each of 48- bit length. It also contains 8 S- boxes and same algorithm is used in reversed for decryption [3]. The implementations of the DES (data encryption standard) algorithm based on hardware are low cost, flexible and efficient encryption solutions.

Algorithm:

DES_ Encrypt (X, Y) where E = (L, R)

X ← IP (M)

\For round ←1 to 16 do

Yi ←SY (Y, round)

L ←L xor F(R, Ki)

swap (L, R)

End

swap (L, R)

X←IP^{-1}(X)

return X.

End

❖ Triple-DES

TDES is an enhanced version of DES is based on Feistel structure. The CPU power consumed by TDES is three times more than DES. The 3DES uses a 64 bit plain text with 48 rounds and a Key Length of 168-bits permuted into 16 sub- keys each of 48- bit length. It also contains 8 S-boxes and same algorithm is used in reversed for decryption [4]. Triple DES the algorithm is considered to be practically secure, in spite of having theoretical attacks.

Algorithm

For j = 1 to 3

{

C**j,0** = IV**j**

For i = 1 to n**j**

{

C**j,i** = E**K3** (D**K2** (E**K1** (P**j,i** C**j,i-1**)))

Output C**j,i**

}

}

❖ Blowfish

Blowfish algorithm was first introduced in 1993.The Blowfish is highly rated secure variable length key encryption algorithm with different structure and functionality than all other algorithms. Blowfish is a block cipher that uses a 64 bit plain text with 16 rounds, allowing a variable key length, up to 448 bits, permuted into 18 sub-keys each of 32- bit length and can be implemented on 32- or 64-bit processors. It also contains 4 S- boxes and same algorithm is used in reversed for decryption [5].

Algorithm

Divide x into two 32-bit lengths : x**L**, xM

For i = 1to 16:

X**L**= X**L** XOR P**i**

x**M** = F (X**L**) XOR x**M**

Swap X**L** and x**M**

Next i

Swap X**L** and x**M** (Undo the last swap.)

x**M** = x**M** XOR P**17**

x**L** = x**L** XOR P**18 then**

Combine XL and x**M.**

❖ RC5

It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow. [5]

Algorithm

A = A + S[0];

B = B + S[1];

for i = 1 to r do

A = ((A Xor B) <<< B) + S[2 * i]

B = ((B Xor A) <<< A) + S[2 * i + 1]

Next

❖ AES

AES is also a symmetric key algorithm based on Feistel structure is developed by Joan Daemen and Vincent Rijmen is new one in October 2000 declared by NIST. The AES is a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 10, October-2018

block cipher that uses a 128 bit plain text with variable 10, 12, or 14 rounds and a variable Key Length of 128, 192, 256 bit permuted into 10 sub- keys each of 128, 192, 256 bit length respectively[7].. It only contains a single S- box and same algorithm is used in reversed for decryption. Rijndael's default number of Rounds is dependent on key size i.e. Rounds = key length/32 + 6. Rijndael AES provides great flexibility for implementing based on parallel structure with effective resistance against attacks [5] [6].

Algorithm

```
Cipher (byte [] input, byte [] output)
{
 byte[4,4] State;

 copy input[] into State[] Add Round Key

 for (round = 1; round < Nr-1; ++round)

 {

   SubBytes ShiftRowsMixColumns AddRoundKey

  }
       SubBytes ShiftRows AddRoundKey

        copy State[] to output []
         }
```

B. Asymmetric Key cryptographic Algorithms

Public-key cryptosystems help solve the key distribution problem by using separate keys for encryption and decryption, and making the encryption key public. One party can encrypt the message with public key (known) and other party processes decrypt message with private key (unknown). Public key systems rely on one-way trap door functions, which are interesting mathematical functions that can be easily computed in one direction but are very difficult to reverse unless a secret key is known (the trap door).

- RSA
- DSA
- Diffie-Hellman
- ELGAMMAL

❖ RSA ALGORITHM

Rivest-Shamir-Adleman (RSA) is a special type of public key cryptography which over the years has reigned supreme as the most widely accepted and implemented general-purpose approach public-key encryption techniques [4]. The RSA algorithm follows a block cipher encryption technique, in which the plaintext and the cipher are integers between 0 and n – 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than to1024.RSA algorithm has three major steps.

1. Key generation
2. Encryption
3. Decryption

Algorithm

1. Key Generation; KeyGen (p,q)

Input : Select two prime integers p ,q.

2. Compute $n = p\,q$, $\Phi(n) = (p-1)(q-1)$

3. Choose e as exponent then gcd (e, p-1) = 1

4. gcd (e, q-1) = 1

5. gcd (e, (p-1) (q-1)) = 1

6. Compute d such that $ed \equiv 1 \pmod{\Phi(n)}$

7. Compute $d = e^{-1} \pmod{\Phi(n)}$

Find a unique value d such that

$\Phi(n)$ divides 5d-1 value ---- pi Key

Public Key = (n, e).

Private Key = (n, d).

Encryption

$C \equiv M^{E} \pmod{N}$

8. Encrypt the message M

$C \equiv M^{E} \pmod{N}$

Decryption

9. To decrypt the cipher text we have

$M = C^{d} \pmod{n}$

M = Plain Text.

❖ DSA

The Digital Signature Algorithm (DSA) was proposed by the National Institute of Standards and Technology (NIST) in August 1991. DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [6]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. [7]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 10, October-2018

❖ Diffie-Hellman Key Exchange (D-H)

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

❖ EIGamel

In cryptography, the EIGamel encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher EIGamel in 1984. EIGamel encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the EIGamel signature scheme, which should not be confused with EIGamel encryption. EIGamel encryption can be defined over any cyclic group .Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms.

IV. PROPOSED MODEL FOR SECURITY IN CLOUD

RSA key generation is the initial stage wherein two keys are generated using various methods that would be further used for encryption and decryption purpose. RSA's encryption products use two keys.

Example: suppose person A send a message to person B. person A uses a Private key that is associated with an encryption algorithm and he wants send/receive encrypted data , he needs to share his public key with the person B wants to send/receive encrypted information

For Example: - Consider a person „A" who possess public key and a private key that is associated with an encryption algorithm, if he wished to send/receive encrypted data, he needs to share his public key with the person he wants to send/receive encrypted information. Using encryption the public key is wrong between A and B or in a cloud number of users. In addition person „A" could send two pieces of information, one original and other scrambled. When this information is decrypted and they match, it guarantees that the information is genuine and has not been tampered. Thus RSA not only secures the data, but also authenticates the sender's identity, which verifies the integrity of received data.

A.Enhanced RSA algorithm

The proposed algorithm has also three major steps

1.Key Generation using big or large integers

2.Encryption

3. Decryption

We can avoid above problem to implement the Decryption with Big Integers of 2' Complement using Chinese Remainder Theorem.. In Decryption may be to representation of 2'complement form of the big integers to splitting the encrypted data two computations.

$M = C^d \pmod n$

Pair of public key = (e,N)

Pair of private key = (p,q, dp,dq)

The CRT is $x_1 = a_1 \pmod{n_1}$

$x_2 = a_2 \pmod{n_2}$

.
.
.

$X_n \equiv a_r \pmod{n_r}$

$M_p = C^{dp} \pmod p$

$Mq = C^{dq} \pmod q$

Similar to CRT i.e.

$M = (Mpq\ (q\text{-}1 \bmod p) + Mqp\ (p\text{-}1 \bmod q)) \bmod N$

So the decryption process may split encrypted data into two computations. So the decryption processes may be faster than RSA Algorithm.

V. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS

RSA, a cryptographic algorithm whose encryption key is public and differs from the decryption key which is kept secret. Data Encryption Standard (DES) and Simplifies Data Encryption Standard (S-DES), where DES used symmetric key for encryption and decryption. Secure Socket Layer (SSL) 128 bit encryption, it is commonly-used protocol for managing the security of a message transmission on the Internet and it uses public and private key encryption system. Mixed encryption algorithms.RC5 which is a symmetric key block cipher and it consists of a number of modular additions and Exclusive OR (EXOR).

VI. CONCLUSION

Cloud computing is latest development that provides easy access to high performance computing resources without installation of software. It provides many benefits for its users but it suffers with some security threats. Security of data is one of the top list impediments in the growth of this latest technology. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of DES, 3DES, AES, RSA, IDES, Blowfish..

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 10, October-2018

REFERENCES

[1] NIST SP 800-145, “A NIST definition of cloud computing.

[2] NIST SP 500-292, "NIST Cloud Computing Reference Architecture.

[3] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou “Ensuring Data Storage Security in Cloud Computing.” IEEE 2009.

[4] Yogesh Kumar, Rajiv Munjal andn Harsh Sharma Comparison of Symmetric and Asymmetric Cryptography With Existing Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and anagement Studies, Vol. 11, Issue 03, Oct 2011.

[5] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,“ Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA Volume 8, 2009.

[6] Gurpreet Singh, Supriya Kinger”Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security “International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[7] Uma Somani, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[8] T V Sathyanarayana and Dr. L. Mary Immaculate Sheela "Data Security in Cloud Computing", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE) 2013, pp 810-813, 14362505/2013.

[9] Cong Wang, Qian Wang and Kui Ren,”Ensuring Data Storage Security in Cloud Computing” 978-1- 4244 – 3876-1/2009 IEEE.

[10] Siani Pearson “Taking account of Privacy when Designing Cloud computing Services CLOUD‟09”, May 23, 2009, Vancouver, Canada, 2009 IEEE.

[11] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, “On technical security issues in cloud computing” 2009, IEEE Computer Society .

[12] Pachipala Yellamma, Challa Narasimham, Velagapudi Sreenivas, “DATA SECURITY IN CLOUD USING RSA” Computing Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference, pp.1-6, 978- 1,2013.