ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Providing Better Security in Cloud Computing Environment using Twofish Encryption

Hemalatha K.L. [1], Sreevathsa C.V. [2]

Associate Professor & Head of the Department, Department of ISE, SKIT, Bengaluru, Karnataka, India[1]

U.G Student, Department of ISE, SKIT, Bengaluru, Karnataka, India[2]

ABSTRACT: This is an era where new technologies will emerge and cannot be relied on any of these because each and every technology is proven to be vulnerable. In the recent times people have come across new technology called the cloud computing. This has given a big hit because instead of saving a huge amount of data in the host machine, user's can store in a server which is remote. Using this services user's can process and manipulate the data which is stored in remote servers. The main challenge for the user is to encrypt his data when he's storing and decrypt while accessing it. Thus, this paper discusses the security issues related to cloud computing and reduce a kind of attacks such as Denial of Service (DoS) attack.

KEYWORDS: Cloud Computing, Security, Denial of service.

I. INTRODUCTION

Cloud computing is very trending in which it is very flexible for the user where he can use the default configuration or he can demand a service based on his requirements. The main reason user selecting the cloud service is that minimizing the usage cost and many more. Despite of all these features it has many security based issues. One of those is a DoS attack [1] in which attacker can access all the resources of the user by sending fake requests. When the real user try to access the same resource it become unavailable [2]. Encryption and decryption of the data is mandatory [3] those are provided with standard algorithm such as RSA and AES. [4] The AES is used to generate a cipher and encrypt the data and RSA is used to provide private keys for encrypting and decrypting of the data. [9] Blowfish is an algorithm which has fewer constraints and provides good encryption mechanism. The main aspect of this paper is to provide more security and increase the performance using the advanced approach. The new algorithm which can be used is twofish which can be more efficient than the standard AES.

II. RELATED WORK

The DoS Attack is a major threat to the cloud computing services it is process where making the resources unavailable for the users [5] the services which cloud provide such as Software as Services (SaaS) and Platform as Service (PaS) are prone to this type of attack. In this type of attack the attackers send numerous fake requests and try to keep server busy which return invalid address request. So, the main aim to keep the server busy from the user and he cannot get access. This could take place in any websites, email or online transactions etc. To reduce this type of attack a solution was designed [6] called the Cloud Trace Back (CTB) in which the source of this attack can be found and prevent it for a shorter amount of time. If the system are not given any security measures is prone to DoS attack. So, if CTB is added to cloud system the requests are sent to CTB first which validates address of the user and try to reduce the attack to some extent. But this was found not an effective way and should come up with a strong approach so that security can be provided. [7] The algorithms like RSA, DES, and AES were found to be effective based on the analysis that the time taken to encrypt and decrypt. RSA algorithm provides the two keys namely private key and public key. In which public key can be provided to everyone and the latter is secured. The DES is used to secure a block of data which is usually a 64-bit block. AES type of encryption technique is useful in both hardware and software, which usually makes 128-bit blocks and key length, can be of 128,192 and 256 bits. The simulation of these algorithms was made and performances

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

were found good. But the paper [8] gives us a clear picture about the RSA algorithm which is used in the field of Cryptography & Network Security has the best performance and implementation of the same will give a better results. In [9] the authors describe about new techniques such as blowfish which solved the security issues in cloud computing environment and through the analysis it is proven to be more efficient technique. So enhancing the above mentioned technique use of the twofish encryption technique performs better in the non-secured cloud server.

III. IMPLEMENTATION

Twofish encryption technique is successor of blowfish technique and it is a 128-bit symmetric block cipher. The Key length may be of 128 bits, 192 bits, and 256 bits. There are no weak keys. It is very flexible in design which can be used in wide variety of services and applications. Because it offers very less space and work at a greater speed. The specialty is such that it is easy to analyze and to implement. Based on the research it found that it is more secure than the AES.

Some performance criteria are as follows:

1. It can accept any key length up to 256 bits.
2. Encrypted data is less than 500 clock cycles per block on most of the processors.
3. It doesn't include any extra element to make itself as inefficient in hardware.

Fig.1 shows the functional block diagram of the twofish algorithm. The steps involved in the Twofish algorithm as follows:

1. **Keyed S –boxes**: Twofish builds four bijective key-dependent 8x8-bit S-boxes using a key or permutation in the form of sandwich (shown for a 128-bit key):
   s0(x) = q1[q0[q0[x] ^ k0] ^ k1]
   s1(x) = q0[q0[q1[x] ^ k2] ^ k3]
   s2(x) = q1[q1[q0[x] ^ k4] ^ k5]
   s3(x) = q0[q1[q1[x] ^ k6] ^ k7]
   Where q0, q1 are two fixed 8-bit permutations.

2. **MDS Matrix:**
   a) 4x4 matrix multiply over GF(256): v = Mu.
   b) Maximum Distance Separable (MDS) property guarantees that there are at least five non-zero bytes in u and v. This is used as the main diffusion mechanism in Twofish.
   c) The Minimum binary Hamming weight output for single byte input difference is 8 bits. Preserves MDS property for single byte. But the input difference even after single-bit "rotate right" of v (Which is treated as a 32-bit quantity).

3. **PHT:** Pseudo-Hadamard Transform(PHT) is a simple, fast, and reversible diffusion mechanism.
   a' = a + b
   b' = a + b*2
   Twofish uses 32-bit PHT on pairs on MDS outputs.

4. **1-bit Rotation:** It is used in each Twofish round to break up the byte-aligned nature of other operations. All the four 32-bit quantity in the block is used once in each of the eight possible bit positions (mod 8).

5. **Subkeys:** The subkeys are based on same construction as keydependent S-boxes. Can be precomputed or constructed on the fly.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

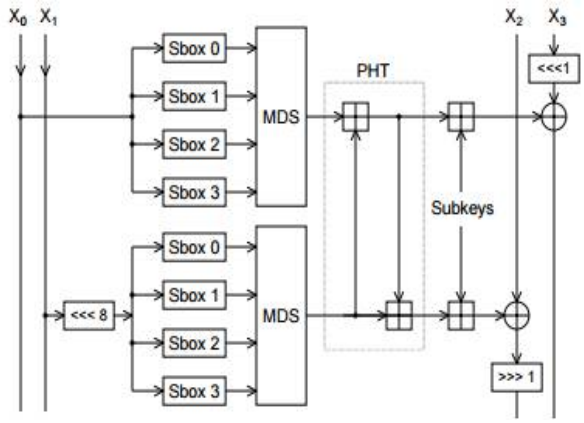

Fig.1. Twofish functional block diagram

IV. EXPERIMENTAL RESULTS

In this proposed system twofish encryption is unbreakable. Thus, it prevents the DoS attack. But the algorithm such as AES can be breakable. Twofish provides some unique keys. Twofish algorithm will not vary the number of rounds for any key size of 128 bits, 192 bits, and 256 bits. Instead, it uses a fixed number of 16. It is very efficient when it comes to hardware. It consumes a very little memory and fewer cycles in order to encrypt data. Twofish consumes very less amount of RAM for its operation to perform, for 128 bits, 192 bits and, 256 bits it requires only 36 bytes, 36 bytes, and 48 bytes respectively. The code size required for this is very less. Hence, it is very compact. The same code can be used for both encryption and decryption.

V. CONCLUSION

From the above implementation it can be concluded that twofish encryption is better algorithm than AES in cloud server because it has unique combination of speed and flexibility. Twofish performs well in all the CPUs. It consumes very less amount of RAM. Thus, the encryption can be made faster and the security is high because twofish can't be broken easily.

VI. FUTURE ENHANCEMENT

Through this paper an attempt has been made to solve some of the security issues in cloud using Twofish encryption technique, which was found more secure and efficient. But there is possibility that there may be some weak keys in the S-boxes. In future to the proposed system, there are upcoming standards to provide security to the cloud server such as threefish and few more which may overcome this problem. So, newer algorithms can be used in place of the proposed system by considering our cloud server to a non-secure one.

REFERENCES

[1] M. Zhou, R. Zhang, W.Xie, W. Qian, & A.Zhou, "Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)", sixth international IEEE conference, Beijing, China,2011.
[2] Z. Muda, W. Yassin, M.N. Sulaiman, and N.I. Udzir, "Intrusion detection based on K-Means clustering and Naïve Bayes classification", 7th International Conference on Information Technology in Asia: Emerging Convergences and Singularity of Forms (CITA), 2011
[3] G.N.Shindeand H.S. Fade War, "Faster RSA algorithm for decryption using Chinese remainder theorem", ICCES, vol. 5, no. 4, 20, pp. 255-261,2008.
[4] Navdeep Singh and Pankaj Deep Kaur, "A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks" , Vol.8, No.3 , pp.145-154,2015.
[5] Q.Guand P. Liu, "Denial of Service Attacks", Department of Computer ScienceTexas State University; School of Information Sciences and Technology,Pennsylvania State University.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

[6] C. Ashle, Y. Xiang, W. Zhou and A.Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks", doi:10.1016/j.jnca.2010.06.004,2010.
[7] P. Mahajan & A.Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security vol. 13, no. 15,2013.
[8] P. S. Yadav, P. Sharma, K. P Yadav, "Implementation of rsa algorithm using elliptic curve algorithm for security and performance enhancement", International Journal of Scientific & Technology Research, vol. 1, no. 4, 2012.
[9] Santhi Baskaran , Surya A , Stephen Pius C , Sudesh Goud G, "Security over Cloud Data through Encryption Standards", ISSN 2250-2459, Volume 5, Issue 3, March 2015.