Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Security in Cloud using Hybrid Encryption and Decryption

HanumanthaRao.Galli*
Research Scholar, CSE Department,
JNTUH University, Hyderabad
Andhra Pradesh,INDIA-500085

Dr.P.Padmanabham
Professor and Director, CSE Department
Bharat Inst. Of Eng. &Tech,Ranga Reddy
Andhra Pradesh, INDIA -501510

Abstract— cloud computing is the new paradigm which provides services on demand from shared pool of computing resources. This new paradigm brings about new security challenges. Cloud is equal with the internet. There are various risk associated with the security but major issues are data privacy and data stealing. This work studies on confidentiality, Integrity and authentication of data storage in the cloud. User has to confirm that the data on the cloud neither compromised nor corrupted, thus makes authentication and authorization for data access is necessary. The proposed method put forward a new security scheme for the files to be uploaded on cloud; it uses hybrid encryption and digital signature scheme. The integrity of the data can be achieved by generating message digest using MD5 algorithm. By using Blowfish algorithm data can encrypted for providing confidentiality. Authentication takes place by RSA algorithm.

Keywords— Cloud computing, Blowfish, RSA, security, encryption, digital signature and data integrity.

I. INTRODUCTION

Cloud is the future of computing. Cloud computing has been defined by national institute of standards and technology (NIST) as Cloud is the network based environment which makes services available on demand. Cloud computing refers to both the applications delivered as services over the internet and the hardware and software in the data centers that provide those services. The best definition for cloud is large pool of easily accessible and virtualized resources which can be dynamically reconfigured to adjust a variable load, allowing also for optimum scale utilization[1].

II. SECURITY ISSUES IN CLOUD COMPUTING

The cloud provider has to ensure that the customer does not face any problem such as loss of data or data theft[2]. There is a chance that attacker can mitigate as a legitimate user, there by effecting the entire cloud[3]. This leads to affects many customers who are sharing the infected cloud[4]. The following are the security issues[5]:

1. *Data Issues*

Whenever data is on a cloud, anyone can access common, private and sensitive data in a cloud from anywhere any time. So that the customer, the cloud provider can modify data.

Data stealing and data loss are the serious issues in a cloud computing environment. These are occurred due to cloud service provider depends on the others server, shutdown of his service due to legal problem etc.

2. *Privacy Issues*

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintain the server so that it enable the provider to protect the customer's personal information.

3. *Infected application*

Any malicious user is uploading any infected application onto the cloud which will affect the customer and cloud computing service.

4. *Security Issues*

Security must be provided on two levels. One is on provider level and another is on user level. The user should make sure that there should not any loss of data or stealing or tampering of data for the other users who are using the same cloud due to its action.

5. *Trust issues*

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

III. ALGORITHMS

The following algorithms are used[9] :

Blowfish

Blowfish is block cipher 64-bit block- can be used as a replacement for the DES algorithm. Its structure is similar to IDEA algorithm[10][11]. It takes a variable length key, ranging from 32 bits to 448-bits [7]. Blowfish is successor of

Twofish. The blowfish algorithm was first introduce in 1993 by Bruce Schneier, and has not cracked yet. It is also noteworthy to point out that this algorithm can be optimized in hard ware applications, although it is like most other ciphers, is often used in software applications. The encryption is simply like feistal network of 16 rounds. For the input of 64 bits, do[12];

Divide data into 32-bit halves: dataL,dataR
For j=1 to 16
dataL=dataL XOR Pj
dataR=F(dataL) XOR dataR
swap dataL and dataR
Next j
Swap dataL and dataR(Undo the last swap)
dataR=dataR XOR P17
dataL=dataL XOR P18
Recombine dataL and dataR.

The F function is: F(dataL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232 where a,b,c,d are four 8 bit quartered derived from dataL.

MD5(Message Digest)

MD5 algorithm developed by Ron rivest and introduced in the year 1991. It is used to verify the integrity of the message. The main goal of this algorithm is security, speed, simplicity, compactness, and little-endian architecture. It processes block of 512-bit and generates 128-bit message digest. The processing consisting of the following steps:

1. Append the padding bits
2. Append the length
3. Initialize MD buffer
4. Process message in 512 bit blocks.
5. Output generation

RSA

RSA algorithm is used for authentication of the message. RSA algorithm was developed by Ron Rivest, Adi Shamir and Leonard Adleman. It is a public key cryptographic algorithm[8], which uses two keys(public key, private key). One key used for encryption and the other key is used for decryption. It requires the following steps[13]:

1. Key Generation
   - Select p and q both prime numbers
   - Calculate n=p * q
   - Calculate $\phi(n)=(p-1) * (q-1)$
   - Select integer e such that $GCD(\phi(n),e)=1;1<e<\phi(n)$
   - Calculate d, $d=e^{-1} \bmod \phi(n)$
   - Public key KU=[e,n]
   - Private key Kr=[d,n]
2. Encryption
   - Plain text M, M<n
   - Cipher text $C=M^e \bmod n$
3. Decryption
   - Cipher text C
   - Plain text $M=C^d \pmod n$

IV. PROPOSED SCHEME

In this scheme it uses both symmetric and asymmetric cryptographic algorithms are used for data storage and transmission over a network[6].

Encryption process

i. A secret key of variable length 32 bits to 448-bits is chosen[7].
ii. Using this key cipher text is generated for the message(M)
   E_M=Blowfish(M).
iii. Blowfish key is encrypted using RSA algorithm
   Ek2=RSA(blowfish key)
iv. The encrypted message is act as input to the MD5 algorithm which generates 512 bit message digest
   E_H =MD5(E_M)
v. The message digest be signed using RSA digital signature algorithm using private key of the sender ,hence generating a digital signature
   D=RSA-Sign(E_H)
vi. The encrypted message(E_M), digital signature(D) and encrypted blowfish key are transmitted across the network.

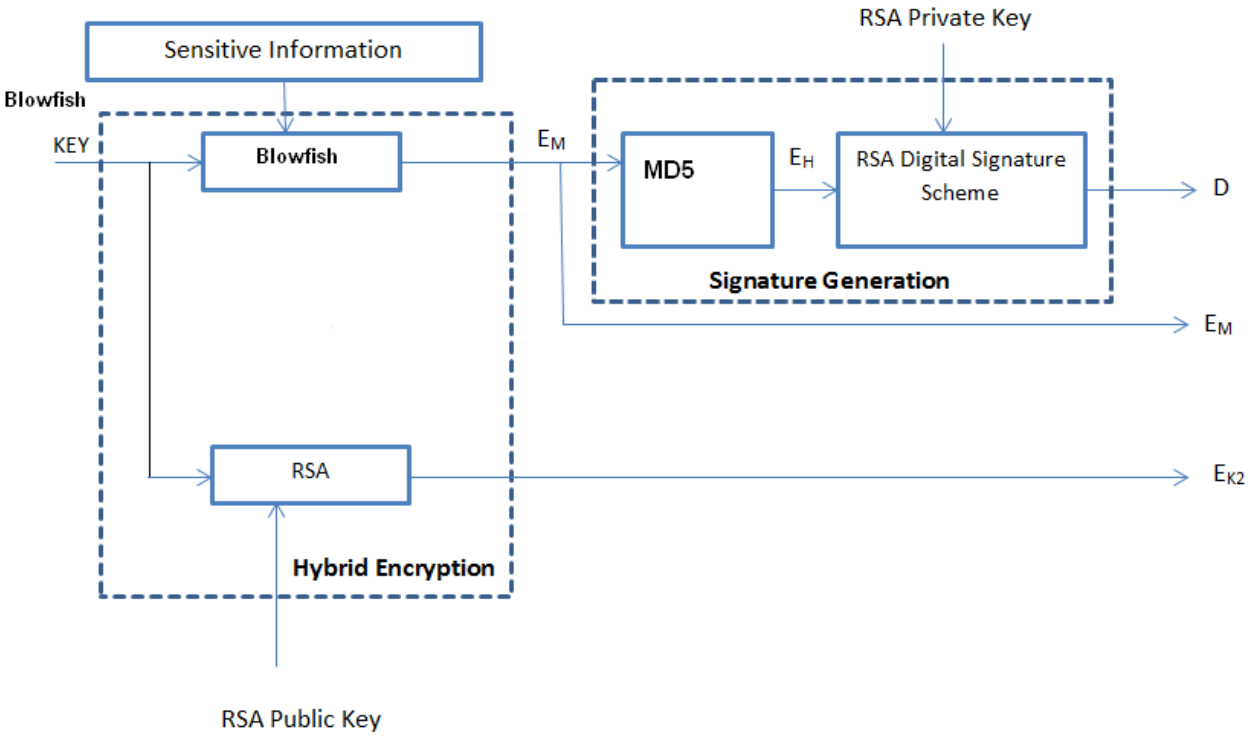

Fig: Encryption process

Decryption Process

The following are the steps for decryption:

i. The encrypted blowfish key(Ek2) is given to RSA decryption which gives blowfish key.
K=RSA-Decrypt(Ek2)

ii. The original message can be obtained by decrypting the cipher text by using the key obtained from above step.
M=Blowfish-Decrypt(E_M)

iii. The encrypted message is act as input to the MD5 algorithm which generates 512 bit message digest
E_H =MD5(E_M)

iv. The digital signature acts as input to RSA digital signature verification algorithm which produces the expected hash (E_H) using sender's public key[14].
E_H =RSA-verify(D).

v. The generated hashes from step iii and step iv are compared.

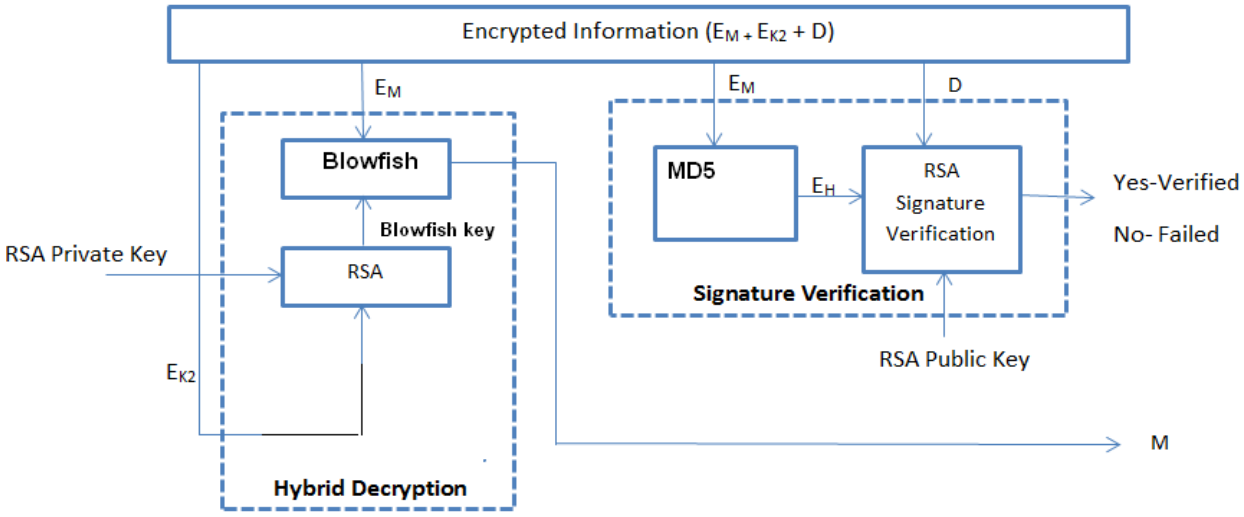

Fig: Decryption Process

V. CONCLUSIONS

A combination of hybrid cryptography and the digital signatures provides a powerful solution to implement services that guarantee data protection and data integrity. Secondly, the two tier encryption of symmetric key further adds to the security. Blowfish algorithm in encryption/decryption process shows high efficiency and ease of implementation. Also, Blowfish uses 128 bit key that is strong enough against various cryptographic attacks. In fact, there are no linear

cryptanalytic attacks on Blowfish and there are no known algebraic weaknesses in Blowfish. RSA algorithm used to encrypt the symmetric key, ensures the safe delivery of symmetric key necessary for encryption or decryption of data. RSA Digital Signature Scheme ensures authenticity and integrity of data.

REFERENCES

[1] P. Subhasri and A. Padmapriya, "Cloud Computing: Security Challenges & Encryption Practices", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, March 2013.

[2] Tanisha , Reema Gupta, Dr. Rajesh Kumar,"File Security in Cloud using Two-tier Encryption and Decryption", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, July 2013.

[3] K. Nafi, T. Kar, S. Hoque and M. Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", International Journal of Advanced Computer Science and Applications, vol. 3, no. 10, 2012.

[4] P.Subhasri,Dr. A.PadmaPriya "Mutlilevel Encryption for Ensuring Public cloud" , International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, July 2013.

[5] Z. Tang, X. Wang, L. Jia, and W. Man, "Study on Data Security of Cloud Computing", Proc. IEEE Spring Congress on Engineering and Technology, pp: 1-3, 2012.

[6] A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering , vol. 4, no. 9, pp:1650- 1657, September 2012.

[7] Vinaya.V, Sumathi.P," Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013.

[8] Y.P. Singh and M. Khan, "On the Security of Joint Signature and Hybrid Encryption", Proc. 13th IEEE International Conference on Networks, vol. 1, 2005.

[9] Leena Khanna,Prof. Anant Jaiswal, "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, March 2013.44

[10] S. Basu, "International Data Encryption Algorithm (IDEA) – A Typical Illustration", Journal of Global Research in Computer Science, vol. 2, no. 7, pp: 116-118, July 2011.

[11] M. Leong, O. Cheung, K. Tsoi and P. Leong, "A Bit Serial Implementation of the International data Encryption Algorithm IDEA", Proc. IEEE Symposium on Field-Programmable Custom Computing Machines, pp:122-131, 2000.

[12] N.Hoffman, "A Simplified Blowfish Algorithm", Journal Cryptologia,.

[13] W. Hui and M. Jun, "Research of the Database Encryption Technique Based on Hybrid Cryptography", Proc. IEEE Symposium on Computational Intelligence and Design, vol.2, pp: 68-71, 2010.

[14] Richa Chowdary,satyakshma rawat," One Time Password for Multi-Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, March 2013.

