A HYBRID DATA ENCRYPTION TECHNIQUE USING TWO FISH AND ELGAMAL FOR CLOUD COMPUTING

M.Vedaraj

Research Scholar, RMD Engineering College, Tamilnadu

Dr.M.Vigilson Prem

Professor, RMK College of Engineering and Technology, Tamilnadu

ABSTRACT

Many services are being provided to the users by the cloud system. The usage of cloud services has become closely associated with common cloud offerings, such as Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). Cloud Computing provides resources to the users over internet as per their demand. Service on demand is an important feature of cloud computing as it enables the user to pay for the required resources only. Google, Microsoft, IBM, Oracle Corporation and Amazon Web Services are some of the Cloud Service Providers (CSP). The most challenging issue in the cloud technology is security.This paper introduces a new hybrid algorithm which is blend of two cryptographic algorithms:Twofish and ElGamal. This new algorithm which is the hybrid of Twofish and Elgamal provides security to the data while it is being uploaded or downloaded from cloud.

Keywords- Cloud Computing, Security, Two fish Algorithm, ElGamal

1.INTRODUCTION

In the present world, the most powerful and evolving networking system which is utilized by developers as well as users is Cloud computing [5]. Providing security in cloud computing plays a prime concern for its effective utilization and is one of the challenging factor in the network platform. Cloud computing environment shares its resources among servers, users and individuals and in turn, the files or data that are stored in the Cloud are openly accessible to all. Due to this open accessibility factor, the files or data of an individual are more vulnerable and are under threat [6,15]. The impact of data misuse by the intruders possesses a major risk. The intruder may destroy or corrupt the original data and may also disrupt the communication. A lot of attention is required by the Cloud service providers on the security of critical applications [13]. One of the common problem in Cloud is that an individual does not possess the control over the place of data storage. Effective security should be implemented in order to overcome the problem of utilization of resource allocation and scheduling facilities by the user which in turn makes the protection of data or files of the individual as an essential part at the time of processing . We have explored variety of security aspects in our proposed Cloud computing model.Till date, researchers have developed different security models and applied algorithms on them, but those models were unable to solve all types of security threats which has been discussed in [14,10,7]. As this is an era of E-commerce [8] and online business, in order to have an effective e-commerce and online business processing systems we are required to imply high capacity security models in Cloud computing environment. Although it is found in [11] that present security models sometimes utilizes secured communication channel, the process is not cost effective. One can hardly find a model which can utilize security in main server as well as in transaction. In [12], the researchers have proposed hardware encryption system for

augmentation of secured communication system but it provides certain drawbacks like i) difficulty in practical implementation , ii) hardware encryption is effective for database system and not for other security issues.

In the current networking environment, authenticated user detection technique plays a vital role but the recently used security models hardly emphasizes on this technique in Cloud environment. In this paper, we have proposed the concept of Twofish and Elgamal for effective handling of authentication and security which can be utilized in Cloud computing environment.

II. RELATED WORK

Dr. Nandita Sengupta[15],"Designing of Hybrid RSA Encryption Algorithm for Cloud Security", state that Cloud system is an emerging technology in which security is the most challenging issue. Hybrid RSA encryption algorithm is proposed in the paper for security of data in cloud system. In the first phase RSA Encryption algorithm will be applied and in the second phase Feistel encryption algorithm will be applied on the output data, i.e., cipher text of first phase. After final phase, encrypted data will be sent for transmission. As the proposed algorithm has two phases, probability of man-in-the-middle attack will be less.

Garima and Naveen [5], "Triple Security of Data in Cloud Computing", state that cloud computing is a networking model which is connected to a number of servers and is based on client server architecture providing various facilities due to its flexible infrastructure. According to this paper, since cloud computing is internet based technology, so, security stands as a major concern and introduce a mechanism to protect the data in the cloud using combination of two cryptographic algorithms and steganography. This paper proposes blend of two cryptographic algorithms, DSA(Digital Signature Algorithm) and AES(Advanced Encryption Standard) and Steganography. DSA is used for authentication purpose, AES is used for encrypting the data and Steganography is used for further encryption. The working involves signing of the data in the first step. The signature is generated by first applying a hash function on the data and this gives compact form of data which is called message digest. The message digest is then signed using sender's private key. Once the message is signed, the data is encrypted along with the signature using AES. Once encryption is completed using AES algorithm, the data is further encrypted using steganography. Steganography hides message along with another media which does attract the attention of the intruder and hence the data is protected. This complete mechanism is implemented on ASP.NET Platform and ensures to achieve authenticity, data integrity and security of data in the cloud. This paper concludes that time complexity of the complete mechanism is high since it is one by one process.

Parsi and Sudha[4], "Data Security in Cloud Computing using RSA Algorithm", state that cloud computing is an emerging technology and is fast becoming the hottest area of research. Cloud computing is effective in reducing the costs and provides on demand services to the users. Since cloud computing is based on the concept of open environment, security stands as a hindrance to the deployment of cloud environments. To provide data security in cloud environment, RSA algorithm has been implemented to provide the same. RSA stands for Ron Rivest, Adi Shamir and Len Adleman. RSA is public key cryptography. In the proposed system, RSA is used for encryption as well as decryption of data. The process involves that the data is encrypted and then uploaded onto the cloud. For decryption of data, data required is downloaded from the cloud, cloud provider authenticates the user and then the data is decrypted. RSA is used to provide authenticated access to intended user only and hence makes the system secure. The working of RSA consists of two keys: public key and private key. Public key is distributed and shared with others while the private key is only available with the original data owner. Thus, Cloud Service Provider(CSP) perform the encryption and decryption is performed by the consumer or cloud user. Hence, once the data is encrypted using public key, private key must be known in order to decrypt the data. RSA

algorithm has three steps: Key Generation, Encryption and Decryption. Key generation is done between CSP and user and then encryption and decryption are performed further. The proposed system provides authenticated access and prevents any intruder access. Hence, the system is made secure.

Jasleen Kaur[18],"Security in Cloud Computing using Hybrid of Algorithms", state that the Proposed Algorithm consists of hybridization of two algorithms: RSA as Digital Signature and Blowfish Algorithm. Digital Signature will provide authentication and non-repudiation to the data while Blowfish will be used for encryption/decryption. Once the document is signed and encrypted using the hybrid algorithm, it will be uploaded onto the cloud provided by Cloud Service Providers (CSP). For decryption, document will be downloaded and then decrypted after authentication using public key.

A. P Shaikh and V. kaul[17], "Enhanced security algorithm using hybrid encryption and ECC",state that this paper propose a hybrid model which uses a combination of two symmetric algorithms enhanced AES and Blowfish for data confidentiality, Message Digest-5 for data integrity, Elliptic Curve Diffie Hellman algorithm- ECDHA for key exchange and Elliptic Curve Digital signature algorithm-ECDSA is used for digital signature. In this, AES is enhanced by modifying the S-boxes columns, and then the combination of enhanced AES and blowfish is used for data confidentiality. Performance of this system is evaluated on the basis of encryption/decryption time, throughput and memory usage for different data formats like text file, image file, audio file and video file

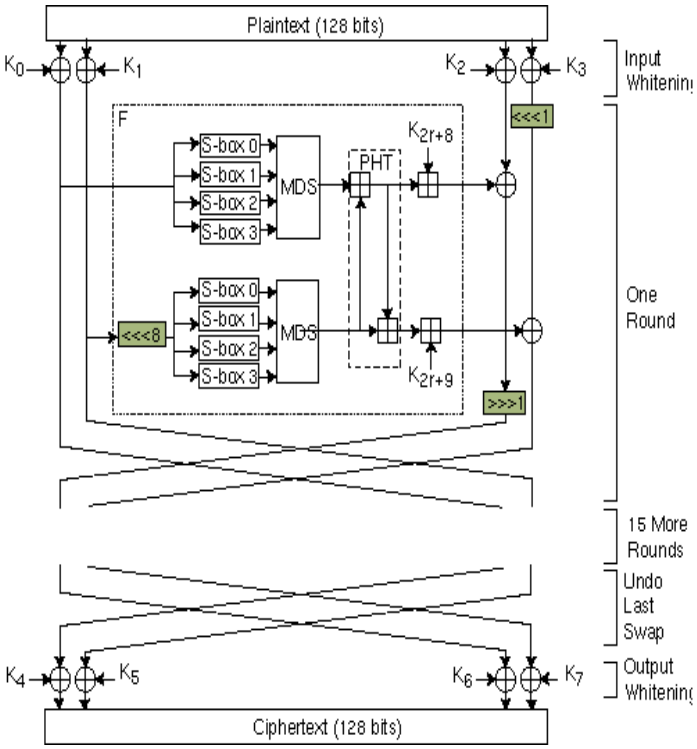
III. PROPOSED SYSTEM

The proposed work is based on blending two popular encryption algorithms ,Twofish and Elgamal algorithm.

TWOFISH

Twofish is a 128-bit block cipher that accepts a variable-length key up to 256 bits. The cipher is a 16-round Feistel network with a bijective F function made up of four key-dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum distance separable matrix over GF(28), a pseudo-Hadamard transform, bitwise rotations, and a carefully designed key schedule.

- The plaintext is split into four 32-bit words.
- In the input whitening step, these are XOR ed with four key words.
- This is followed by sixteen rounds. In each round, the two words on the left are used as input to the g functions.
- The g function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on an MDS matrix.
- Each S-box takes 8 bits of input, and produces 8 bits of output.
- The four results are interpreted as a vector of length 4 and multiplied by the 4X4 MDS (maximum distance separable) matrix.
- The results of the two g functions are combined using a Pseudo- Hadamard Transform (PHT), and two keywords are added.
- These two results are then XOR ed into the words on the right (one of which is rotated left by 1 bit first, the there is rotated right afterwards).
- The left and right halves are then swapped for the next round.
- After all the rounds, the swap of the last round is reversed, and the four words are XOR ed with four mo**re key words to produce the cipher text[19].**



ELGAMAL:

In cryptography, the ElGamal 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 Elgamal in 1984.ElGamal 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 ElGamal signature scheme, which should not be confused with ElGamal encryption.

ElGamal encryption can be defined over any cyclic group G. Its security depends upon the difficulty of a certain problem in G related to computing discrete logarithms.

IV. WORKING OF PROPOSED ALGORITHM

The proposed algorithm based on hybrid of twofish and Elgamal which improve the security of cloud data.

Step1: Encryption using Twofish

a) For encryption, Twofish algorithm is used.

b) The plaintext is split into four 32-bit words, In the first step of input , these are XOR with four k words of expended key.

c) The two words on the left are used as input to the g functions after the rotation by 8 bits of one of them.

d) The g function consist of four byte wide key dependent s-boxes, followed by a linear mixing step based on the MDS matrix.

e) The result of the two g functions are combined using pseudo hadamard transform (PHT), and two keywords are added.

f) One of the words on the right is rotated by bit and then both of them are XOR in to the result on the left.

g) The left and right halves are then swapped for the next round.

h) After 16 rounds, the swap of the last round is reserved, and the four words are XOR ed with four more key words to procedure the cipher text

Step 2: Re-Encrption using ElGamal

a) The keys are generated by selecting a large prime number p.

b) It is recommended that p-1 be divisible by another large numbers

c) Compute a generator number g and select a random integer "a" less than p-1

d) With these numbers compute $b=g^a \pmod p$

e) The public key consists of the three numbers (p,g,b) and the secrete key is the number a.

f) Choose a random k in the range $1 < k < p - 1$.

g) Compute $c_1 = g^k \bmod p$

h) Compute $c_2 = mb^k \bmod p$

i) Return ciphertext (c_1, c_2).

Step 4: Decryption using ElGamal

a.) For decryption Compute $m = c_1^{p-b-1} c_2 \bmod p$

Step 5:Re-Decrption using Twofish

a.) The message can be decrypted again using Twofish.The decryption process is achieved using reverse of Twofish algorithm.

V.CONCLUSION

Cloud computing is fast becoming popular in IT field and is being adopted by every organization in order to keep their data all at one place. Therefore, security of data is an important aspect of cloud computing and can be accomplished by the new hybrid algorithm. Two fish algorithm will provide security by encrypting the data. As the encryption process of Two fish algorithm is complex and cannot be broken easily and also ElGamal encryption is probabilistic, meaning that a single plaintext can be encrypted to many possible ciphertexts, with the consequence that a general ElGamal encryption produces a 2:1 expansion in size from plaintext to ciphertext. the chances of breach in this hybrid algorithm will be quite less So, the hybrid algorithm aims at securing the sensitive data of every organization that is being uploaded onto the cloud.

REFERENCES

[1] Ravi Shankar Dhakar, Amit Kumar Gupta, "Modified RSA Encryption Algorithm (MREA)". Advanced Computing & Communication Technologies (ACCT), Second International Conference, 2012.

[2] Maryam Savari, Mohammad Montazerolzohour and Yeoh Eng Thiam, "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application". Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference, 2012.

[3] P.R. Vijayalakshmi, K. Bommanna Raja, "Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol". Computing, Communication and Applications (ICCCA), International Conference, 2012.

[4] Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." IJRCCT 1.4 (2012).

[5] Saini, Garima, and Naveen Sharma. "Triple Security of Data in Cloud Computing." International Journal of Computer Science & Information Technologies 5.4 (2014).

[6] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011.

[7] Ngongang Guy Mollet, "CLOUD COMPUTING SECURITY", Thesis Paper, April 11, 2011.

[8] Gunasekar Kumar, Anirudh Chelikani, "Analysis of security issues in cloud based e-learning", Master's thesis, 2011.

[9] Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang "Recent Advances in Cloud Security", JOURNAL OF COMPUTERS, VOL. 6, NO. 10, OCTOBER 2011.

[10] "Cloud Computing: Silver Lining or Storm Ahead?", Volume 13 Number 2, Spring 2010.

[11] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy, "Token - Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency", TRUST 2010, LNCS6101, pp . 417–429, 2010.

[12] Trusted Computing Group, "Solving the Data Security Dilemma with Self-Encrypting Drives", May 2010.

[13] Ye Hu, Johnny Wong, Gabriel Iszlai, Marin Litoiu, "Resource Provisioning for Cloud Computing", IBM Canada Ltd., 2009.

[14] Daniele Catteddu, Giles Hogben, "Cloud Computing:- Benefits, risks and recommendations for information security", November, 2009.

[15] Dr. Nandita Sengupta "Designing of Hybrid RSA Encryption Algorithm for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2015.

[16] Jasleen Kaur,"Security in Cloud Computing using Hybrid of Algorithms" International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015.

[17] A. P Shaikh and V. kaul, "Enhanced security algorithm using hybrid encryption and ECC", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 80-85.

[18] Jasleen Kaur[1], Dr. Sushil Garg[2]," Security in Cloud Computing using Hybrid of Algorithms", International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015 ISSN 2091-2730.

[19] G. Kishore Kumar1 , Dr. M. Gobi2," Comparative Study on Blowfish & Twofish Algorithms for Cloud Security" International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 3 Issue 9, September 2017 pp. 1 – 11.