A STUDY OF CLOUD COMPUTING-BASED, SECURE USING CRYPTOGRAPHY TOWARDS FILE STORAGE

PRIYA RANJAN PRIYADARSHI

Research Scholar, Dept. of Computer Application,

Sri Satya Sai University of Technology & Medical Sciences,

Sehore, Bhopal-Indore Road, Madhya Pradesh, India.

Dr. Jitendra Sheetlani

Research Guide, Dept. of Computer Application,

Sri Satya Sai University of Technology & Medical Sciences,

Sehore, Bhopal Indore Road,Madhya Pradesh, India.

ABSTRACT

Currently cloud computing helps in storing huge amounts of data in related to various fields such as manufacturing, military schools, etc. Upon request from the client, the data are collected from the cloud. In order to store information on the cloud, there are several challenges, the solution to these problems are provided by the Cryptography and steganography techniques. The high-level data protection in cloud computing is to use algorithm in unsuccessful. In this paper, we introduced a new safety mechanism using symmetric key cryptography algorithms and steganography. Blowfish, RC6 and BRA algorithms are used in this proposed system to provide data with block wiseprotection. For key information protection, all main algorithm size is 128 bit. LSB steganography technique is implemented. Key information includes that part of the file is encrypted by splitting the algorithm and key. File into eight sections. Using different algorithms, each part of the file is encrypted. Both portions of the file are simultaneously encrypted using the technique of multithreading. Data encryption Using LSB technique, keys are inserted into the cover image. Stego picture is sent by email to a legitimate recipient. Reverse encryption method is implemented for file decryption purposes.

KEYWORDS: Cloud service provider(CSP), encoding, decoding, blocking, integrity.

INTRODUCTION

The methodology of cryptography converts the original data into unreadable form. The methodology of cryptography is divided into symmetric key cryptography and the cryptography of public key. Use keys to convert information into unreadable form, this technique. Just licensed entities can access data from the cloud server. For all men, cipher text information is available.AES, DES, 3DES, IDEA, BRA and blowfish are symmetric key cryptographic algorithms. The main problem is to transmit the receiver key to a multi-user request. Such algorithms require low delay but provide poor security for data encoding decoding. The RSA and ECC algorithm is the public key cryptography algorithm. Public and private keys were incorporated into algorithms for public key cryptography. Such algorithms have achieved a high level of security but are increasing the lag for data encoding and decoding. Steganography conceals the presence

of secret data into the container. Software life is not clear to all people in this technique. Only the legitimate receiver knows the presence of the information.

The technique of text steganography is used to produce high data security. Hidden user data are covered in the folder of the document cover. It looks like a normaltext file after adding text to the data cover file. When text file is discovered by unlawful client, sensitive data cannot also be accessed. If unauthorized client tries to retrieve original data as long as it takes. DES algorithm is used for encoding and decoding text. The benefit of the technique of text steganography is to provide text protection. For text steganography, minimum spaceis necessary compared to photo steganography [2].Three bit LSB technique for steganography of the image. Writer R.T.Patil. Sensitive user data hides this program in the cover image. Use LSB steganography technique, we can conceal huge amounts in image. The author Klaus Hafmann has introduced high-performance architecture for cryptography algorithm. AES is symmetric key algorithm for cryptography.

Three types of keys are supported. For 128-bit key, 10 rounds are needed, 192-bit key, 2 rounds, and 256-bitkey, 14 rounds. In improved AES algorithm encryption and decryption time is reduced. The benefit of modified AES algorithm provides better delay performance [3][4].

Writer M presents a new algorithm for symmetric key cryptography. Nagle. This uses a single key for encoding and decoding documents. Core size is 128 bits. Several steps are performed arbitrarily in this algorithm so unauthorized users can even guess the logarithm steps. One of the benefits of symmetric key cryptography algorithms is to provide high throughput. [5] For data encoding and decoding, the enhanced DES algorithm uses 112 bit key size. DES algorithm input is split into two parts. Those two sections are executed at the same time. DES algorithm has one disadvantage. This is less important size.3DES algorithm requireshuge amount of time for encryption and decryption. Improved DES algorithm has

the ability to deliver better performance compared to DES and 3DES.[6]Name Based Encryption Algorithm operates on one byte at a time. Using the random key generation method, it uses the secret key for encryption and decryption. It gives data security. The downside of this algorithm is that it operates on a single byte at a time[7]To solve data storage and security problems, the author has a new security design. Privateand public cloud storage areas are used in this design to improve data security. Safe data is stored in the private cloud and redundant data is stored in the public cloud. Because anybody can access the public cloud. The main reason behind this program is to reduce storage costs. Private cloud is cheaper than the public cloud.[10]In order to improve information protection in cloud computing. Source data splits into different parts. Every part of the file is encrypted and stored in a cloud. File information is stored for decryption purposes on the cloud server. If the attacker attempts to recover the original file, only one section of the file will be obtained.[11]The Elliptic Curve cryptography algorithm is used to achieve high-level security. Key complexity control is avoided using access management and identity. The ECC algorithm requires total file encoding and decoding time. [12]File is translated from AES algorithm to unreadable format. Encrypted file is stored on the algorithm of cloud. AES is less reliable than the algorithms of public key cryptography. [13] AES and 3DES algorithms are combined into hybrid algorithms to achieve confidentiality. Recovering user's hidden file is more difficult for the attacker. It requires total lag in converting information into decoding and encoding form [14].For data encoding and decoding purposes, a single algorithm is used inthe existing system. Nevertheless, using a single algorithm does not achieve highthe existing system. Nevertheless, using a single algorithm does not achieve high-level security. If we use a single symmetric key cryptography algorithm, we have to face security issues because a single key for data encoding and decoding is used in this type of algorithm. Key transmission problem arises when key is exchanged in multi-user environment. Public key cryptography algorithms achieve high security but for data encoding and decoding, maximum delay is needed. We also introduced a new security mechanism to address the above problems. The owner of the cloud and the client of the cloud are included in the system architecture as shown above in fig 1. Cloud owner upload information to the cloud server. The file is split into a byte. Every part of the file is encoded using multithreading technique simultaneously. Encoded file is stored on the database of the cloud. Keys are contained in the cover image for authentication. Cloud computing is the multi-user system. More than one user can access cloud database file in this environment. Cloud user request for data. Use email, which consists of key information, you will also receive stego picture at the file user's request. To decode the folder, the reverse process is used.

REVIEW OF LITERATURE

A. Triple security of Data in Cloud Computing [8]:

In this paper, the author uses a triple algorithm such as DSA, DES, and Steganography to provide data security for cloud computing. DSA is used in the cloud to authenticate and validate information. DSA is responsible for ensuring information accuracy, honesty and originality. DES is built on an algorithm of symmetric key and is used for data encryption. To ensure security in the cloud, Stenography is used to conceal the information in the audio file. The main drawback in this paper is that time complexity is high due to one by one operation, first applying DSA algorithm for authentication and then applying AES algorithm and stenography process for encryption method. Reverse all system on the receiver side for decryption process so that time complexity is small.

B. Enhancing Data storage Security in Cloud Computing through Steganography [9]:

The author used steganography technique in this paper to allow unauthorized cloud access to data. This improved form of steganography is used to store data in cloud data storage, and when needed, recovers data from the data center. The drawback in this paper, the proposed scheme will address a limited number of threats to security.

C.Data Security in Cloud Computing using Encryption and Steganography [10]:

The writer used the strong AES encryption algorithm in this paper to encrypt the data chosen by the client and then upload it to the database. Next, the hiding algorithm is applied to the encrypted data and stored in the database, and the procedure is reversed to decrypt the data and retrieve the original data. The scheme proposed is used to solve the issue of data security.

D. Enhancing security in cloud computing structure by hybrid encryption [11]:

In this article, the writer proposed the hybrid approach using AES and MD5 algorithms with the idea of white text. The plain text comprises the text to be encrypted and the content of the plain text is translated to the white text. This paper provides the message with the authentication in the form of the hash functionto provide better security in the cloud environment. This scheme is used in the cloud service world to avoid insider attacks.

E. Secure file storage in cloud computing using hybrid cryptography algorithm [12]:

In this paper, using the Symmetric key cryptography algorithm and steganography, the author proposed a new protection mechanism to protect data in the cloud. The combination of four algorithms (AES, blowfish, RC6, and BRA) for high-level data protection in the cloud was used in this proposed scheme and the LSB steganography technique was used for key information safety.

F. Three Step Data Security Model for Cloud Computing based on RSA and Steganography techniques. [13]:

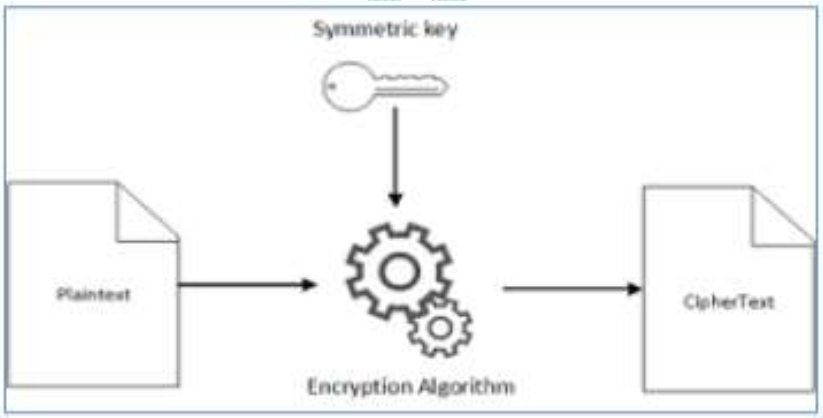
The researchers suggested in this paper a technique of cryptography and steganography to protect information in the cloud while data is stored and exchanged. The first security step is to use the technique of cryptography to encrypt the data. The RSA algorithm is used for the process of encryption and decryption and RSA key generation. The second step is used to conceal the encrypted data using steganography's image data hiding technique. The algorithm used for good cloud and web security in the journal.

G. An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique. [14]:

In this paper, the researchers proposed to use cryptography and steganography and hash function to boost data security in the cloud. Blowfish algorithm is used for cryptography to improve data security and a new powerful embedded algorithm is used for steganography using Embedded Least Significant Bit (E-LSB) and SHA256 Hashing algorithm is used for integrity verification. To order to assess the safety of the steganography process, data destruction attack and data detection are implemented.

Symmetric Key Cyroptography:

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).

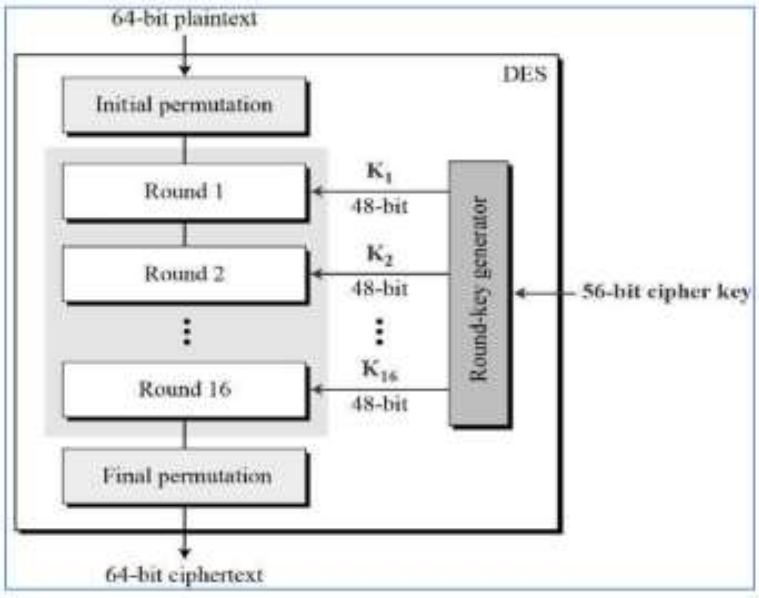


Asymmetric Key Cyroptography:

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie–Hellman and DSA are related to the discrete logarithm problem. More recently, elliptic curve cryptography has developed, a system in which security is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes.

Data Encryption Standard:

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits. The key is nominally stored or transmitted as 8 bytes, each with odd parity. Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes—the only difference is that the subkeys are applied in the reverse order when decrypting.



Advanced Encryption Standard:

AES is a subset of the Rijndael cipher developed by Belgian cryptographers, VincentRijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. A. Byte Substitution (SubBytes) The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns. B. Shiftrows Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

C. Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

D. Add round key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

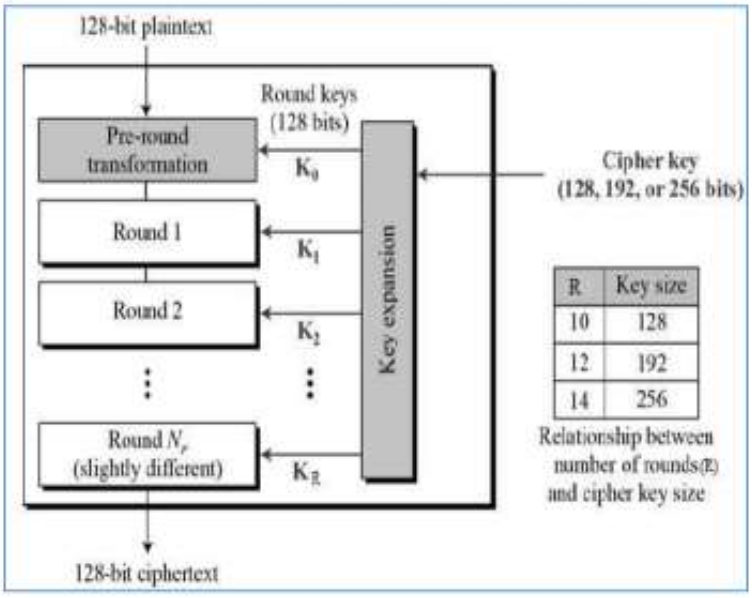
E. Decryption Process

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

- Add round key
- Mix columns
- Shift rows

• Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related



R	Key size
10	128
12	192
14	256

RC-2 Encrypion Algorithm:

In cryptography, RC2 (also known as ARC2) is a symmetrickey block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5, and RC6.

The development of RC2 was sponsored by Lotus, who were seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989.

CONCLUSION

Cloud storage problems are solved using techniques of cryptography and steganography. Block wise Protection of information is accomplished with algorithms AES, RC6, Blowfish and BRA. Main protection of data is done using LSB technique. Using the SHA1 hash algorithm, data confidentiality is achieved. Using multithreading technique, a small delay parameter is achieved. Data integrity, high protection, low latency, encryption and confidentiality criteria are achieved with the aid of the proposed security mechanism. Using the proposed encryption of the text file would take 17% to 20% less time compared to the AES algorithm. The decryption of AES text requires a maximum time of 15 to 17 percent relative to the proposed system. In Blowfish, the maximum time needed for encryption is 12 to 15 percent compared to the proposed hybrid algorithm. The decryption of text files using a hybrid algorithm takes 10% to 12% less time compared to the Blowfish

algorithm. Try to achieve high-level security in the future by hybridizing algorithms for public key cryptography.

REFERENCES

[1] V.S. Mahalle, of course. K. Shahade, "Improving Cloud Data Protection by Hybrid (Rsa&Aes) Encryption Algorithm," IEEE, INPAC, pp 146-149,Oct.2014.

[2] Abu Marjan, PalashUddin, "By Text Steganography and Cryptography, Developing Efficient Information Solution," IEEE, IFOST, pages 14-17, October 2014.

[3] P. S. and R. Bhendwade. T. Patil, IEEE, International Conference on Communication and Signal Processing, pages 953-956, April 2014.

[4] This is S. Hesham and Klaus Hofmann, "Advanced Encryption Standard Algorithm High Throughput Architecture," IEEE, International Symposium on Electronic Circuits & Systems Technology and Diagnostics, pages 167-170, April 2014.

[5] M. Nagle, D. Nilesh, "The High Throughput New Cryptography Algorithm," IEEE, ICCCI, 1-5,January 2014.

[6] DES-based symmetric encryption algorithm design and implementation, Zhou Yingbing, LI Yongzhen, IEEE, ICSESS, pages 517- 520, June 2014.

[7] N. No. Sharma, A. Hasan, "A New Approach to Encryption Schemes (NameBased Encryption Algorithm),"IEEE, International Conference on Reliability, Optimization and Information Technology, pages 310-313,Feb 2014.

[8] Inder Singh, M. Prateek, "Data Encryption and Decryption Algorithms Using Key Rotations N. Sharma, A. Hasan, A New Approach For Encryption Schemes, IEEE, International Conference on Reliability, Optimization and Information Technology, pages 310-313, Feb 2014.

[9] Jasleen K., S. Garg['Cloud Computing Safety using Algorithm Hybrid', IJERJS, Volume 3, Issue 5, ISSN 2091-2730, pages 300-305, September-October 2015.

[10] Jasleen K., S.Garg['Cloud Computing Security using Algorithm Hybrid', IJERJS, Volume 3, Issue 5, ISSN 2091-2730, pages 300-305, September-October 2015.

[11] This is S. Munjal1, S. Garg, "Enhancing Cloud Computing Infrastructure Data Security and Storage," IJCSIT, Vol. 6, ISSN 0975-9646, pages 2623-2626,2015.

[12] U. Veeresh, S. P. Kumar, IJCERT, Vol. "Multi Cloud Infrastructure to Provide Security and Inegrity" 2, Issue 9, ISSN 2349-7084, PP 558-564, September 2015.

[13] This is S. Ali Abbas, "Enhancing Identity Protection and Cloud Access Management with Elliptic Curve Cryptography," IJERMT, Volume-4, Issue-7,ISSN: 2278- 9359, pages 8-15,2015.

[14] Kiruthika. R, Jeena. R, "Improving the security of cloud computing using AES algorithms," IJARCSSE, Volume 5, Issue 3, ISSN 2277 128X, pp 630-635, March 2015.

[15] P. Kanchan, "Use of Digital Signature to Improve Data Security in Cloud Computing with Diffie Hellman Key Exchange and Hybrid Cryptographic Algorithm," Volume 5, Issue 6, ISSN 2250-3153, pp 1-4, June 2015.