

CONSERVATION OF CLOUD STORAGE SECURITY USING HYBRID ALGORITHM

¹Judy Flavia.B, ²P.Visalakshi

¹Final year M.Tech(CSE) student, ²Assistant Professor(Selection Grade)

^{1,2}Department of Computer Science and Engineering,

SRM Institute of Science and Technology, Kattankulathur, Kancheepuram Dist- 603 203

¹flaviacifford@gmail.com, ²visasan2003@gmail.com

Abstract: In this era the quantum of data that are processed are immeasurable. Hence storing this vast amount information in cloud leads to immense security issues. In existing system the security of the system compromised by using linear coding algorithm which affects the data that has been sent through intermediate routers and results in modification of data or data lost. Hence to provide a high security to information in cloud computing, single algorithmic program are not enough. Use of one algorithmic program is not effective for top level security to information in cloud computing. In this paper, we have introduced new security mechanism using interchangeable key cryptography rule. In this methodology, AES and Triple DES algorithms are accustomed give block wise security to information rather than network coding which causes pollution in the code words of the received packets and results in pollutant attack. All algorithmic program key size is 128 bit. The choice of algorithmic programme can occur rely upon the method temporal order. Before applying the rule the data are split into eight components and therefore the numbers are generated indiscriminately according to the time. Within the output size the decipherment method can occur at the same time. The user must apply decipherment key so as to decipher the information on downloading the data. To check the integrity and authenticity of the data that has been stored in the cloud we also use Third party audit. They are also restricted to only view the certain keywords that are allowed by the user.

Keywords: CSP (Cloud storage provider), TPA (Third party audit), Cloud data sharing, Pollutant attack, Cloud storage.

1. Introduction

Cloud computing has been employed in several areas like trade, military education, companies etc. for storing amputee amount of information. Were these data are able to be retrieved on request from users. While storing information on cloud several problems are to be faced. But mainly there are huge risk of data loss during

online sessions in third party cloud storage because of software and hardware failures. Also there is a huge risk due to hackers while retrieving the information. To overcome these issues encryption technique is used while the data's are stored this makes the data less vulnerable. In the traditional method TPA (Third party audit), the user can check the data integrity, pollutant attacks caused by random key generation from the usage of linear encoding algorithm on encryption. In the proposed work hybrid algorithms are used in symmetric key encryption to avoid any random key generation that causes the pollutant attack. In the proposed paper AES and Triple DES algorithms are used by random selection to the time, in which each module is uploaded in the network based on odd and even time spaces

2. Related Work

[1] In this paper linear encoding algorithm is used for secure cloud storage and networking. However this leads to waste attack in the original data. [2] This paper shows Third Party Auditing (TPA) which is employed to visualize the integrity of the outsourced information. It shows how privacy conserving is projected for a secure cloud storage. The disadvantage of this paper is privacy protection of user information against external auditors [3] This work totally different weight are given to negligible the network committal for written problems and is concentrated to short in Pseudo dual graph. The drawback is that the delay and heterogeneousness tie up. [4] In this paper the PANDA method is hired as an auxiliary public auditioning tool for maintaining the reliability of the communal information with economical user annulment in cloud storage. They use batch examining to authenticate multiple auditing tasks at the similar period. Their flaw is low potency in user revocation. [5] This paper shows Hybrid (RSA & AES) cryptography algorithmic program of defence info security of the Cloud. It primarily emphasizes on the following key tasks: 1. Secure transfer of knowledge on cloud that even the administrator is ignorant of the data. 2. Secure transfer of knowledge in a way that integrity of info is upheld. 3.

Precise practice and division of general public, non-public and secret keys concerned in cryptography and decoding. However in hybrid algorithmic program, the hitch is fixed by the utilization of 3 separate keys each for cryptography in accumulation to decoding. [6] This paper deals with the complications of security over indiscreet communication channel. Thus to handle physical time security system they have projected format based pure text steganography algorithm with a private key cryptography which delivers high level of security. Algorithms such as AES, DES, RSA and hash algorithms are used. The drawback of this paper is none of the cover text or steganographical algorithms are not easily available. [7] In this work Steganography is used to overcome the boundaries of information security. Here they suggested network steganography for hiding the information. TCP/IP is used for data masking. Concealed channels steal the info or converse undisclosed info over the network. The disadvantage of the structure is statistical exposure of steganography are not possible due to random transformation plus computation. [8] The progress of internet and wireless communication has a zenith mark on security. Advanced encryption algorithm (AES) has been developed as a new norm for high flexibility and strong security. The proposed architecture in this paper is adapted for encrypted and decrypted schemes which provides competence enhancement of 61%. Its benefit diminishes crucial path delay for both encryption and decryption procedure. [9] The capability to defend the vital information is important in the evolution of e-commerce and internet. Cryptography is logic of mathematical manipulation of figures with some key text. Three main methods in this paper are Key generation, Encryption and Decryption. In the paper 1st new cryptography algorithm is bred and then compared with algorithms like AES, DES, DES, and Blow fish algorithm by components similar to throughput and security is delivered on applying brute force attack. [10] In the work DES is the most noticeable symmetric key algorithm but due to its several inadequacies AES and 3DES algorithms were proposed. They propose two new methods for encryption based on original DES algorithm.

- System with altering outputs.
- System with altering sub keys.

They secure as triple DES algorithm but more complicated and time overshadowing. [11] Name based encryption algorithm (NBE) is a fresh technique that is proposed to increase secrecy of the message without accumulating the complexity of the algorithm. Proposed system uses user defined dynamic key [12] they have proposed an efficient data encryption and decryption algorithm to guard the out sourced delicate information in cloud environs. In encryption of data, user utilizes the aid of file splitting to cut off storage and computational overheads. Trusted TPA is presented for

verification of authorized data from cloud server. [13] This paper presents a new security approach with hybrid algorithms: symmetric and asymmetric algorithms, RSA as Digital Signature and Blowfish Algorithm. RSA as Digital Signature is used for authentication and verification purpose and Blowfish is used for encryption and security resolve. Two keys are used for signing the document: public key and private key. The Algorithm is fast as it revenues only few milliseconds to encrypt and decrypt the messages. [14] To attain trust and security for picture information this paper signifies a unusual approach for secure partitioning. Elementary idea behind it is to cut down the storage cost and to protect the user privacy by eradicating the attributes of the image that are used to recognize the employer. For enhanced security, sensitive data is kept in private cloud and non-sensitive files in public cloud. The two central conceptions of cloud is Virtualization and Abstraction. Virtualization is attained by pooling and sharing of means. Scalability, elasticity and multi-tenancy are the chief structures of virtualization. Abstraction of system implementation details from the user is the major feature of abstraction. Three main processes in this paper are 1) Image capturing, 2) Image segmentation and 3) Image distribution. This model is found in automated billing, traffic supervision, parking lot managing and shadowing. [15] In proposed system, concept of multiple cloud storage laterally with boosted security by means of encryption techniques are implemented, where relatively storing a complete file on single cloud system where they are split into different chunks these chunks are then encrypted while stored in different clouds. In this model, they differentiate four architecture patterns: Replication of application, Partition of application in tiers, Partition of application logic in fragments and Partition of application data in fragments. The main downside is too much expectation on the proposed model. It's also anticipated that the system should be proficient of restoring the information from residual cloud storage in case of failure.

3. Existing concepts

In this paper, they reveal the bond amid secured cloud storage and secured network coding. The two main entities involved here are the user and the Cloud Storage Providers. Secured cloud storage is built on the following three functions viz. (1) Secured Model, (2) High Level Protocol Specification and (3) Understanding Security. Likewise, Secured network coding is based on system model, protocol syntax and security definition. Here the queries are sent from the client to the user. As per the client request related data are given in the form of encrypted code using linear coding through which router sends the linear

combination of data packets. Homographic linear authenticator and random masking technique are employed while TPA checks the integrity of client info. The major drawback of this system is the lack of security and the pollutant attack caused by the use of linear network coding. A random key is being generated by the intermediate router which may easily spread over the entire network as the router encodes all the packets. This results in pollution of the code that causes illegal modification and information loss when data receiver's attempts decode the data.

4. Proposed System

To overcome the problems of the existing system we develop a secure encryption network security using Symmetric key and AES and Triple DES algorithms with random algorithm selection. At first the text file is split into 8 files based on the formula $n=N/8$, where N is the number of lines in the original text file, n is the number of lines to be in the split file. After splitting the file add a to the start of the first file followed by b to the second file and c to the third file and so on. Then random number is generated based on the system time example if the system time is (6:19:28:11) then the generated random number is $6+19+28+11=64$. Hence 64 is even number select AES algorithm otherwise it will choose triple des algorithm. For each part random number is generated separately and algorithm is selected. After these processes the selected algorithm is applied to each part of the split part. A sign is placed for the selected algorithm at the end of the split part and at last these files are stored as a folder. In Decryption it will scan the last character to detect what algorithm is used in that part. Then the decryption algorithm is used according to the one used in that part. At last the first character of each file is scanned and merged it in order based of the first character in the file.

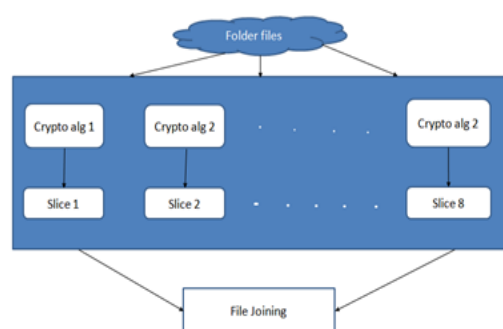


Figure 3.1 File Splitting

The files requested by the clients are retrieved from the cloud storage provider. This file is then split

into eight modules respective to the size of the file and encrypted with AES and Triple DES algorithm.

This paper is consisting of 4 modules which are mentioned as follows:

- Admin Module
- Segmentation and Encryption
- Decryption
- Third Party Audit

In Admin module, the Admin keeps tab of all the data's which are stored. But the admin shall not have any access or authority over the data currently present in that particular storage. In the next module the given data is segmented into eight modules based on the size of the data. After that each module is uploaded to the network depending upon the time using AES and Triple DES algorithm. Then the key is generated using the time space and size of the file decryption algorithm is selected and the data is downloaded. In the final module the client produces a unique user id and password for the third party to check the availability and authenticity of the stored files using large scale text search algorithm.

5. Algorithm Description

In this work various algorithms are used based on the key, which are split into two parts Symmetric Key and Public Key. The symmetric key is consisting of AES algorithm and Triple Data Encryption Standard (DES)DES algorithm. The AES algorithm stands for Advanced Encryption Standard. It is a combination of both substitution and permutation and has a fixed block size of 128 bits, key size of 128,192 or 256 bits. The numbers of rounds are variable and depend on the length of the key. It uses 10 rounds for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys. Each of these rounds uses a different 128 bit round key, which is calculated from the original AES key. The next one is Triple DES Algorithm. It stands for Triple data Encryption Standard. This will first generate and distribute 3TDES Keys, which consist of three different DES keys K_1 , K_2 and K_3 and have a total key length of 168 bits.

In this paper, this algorithm is used to provide an extra addition to the cipher. At first it will encrypt the data's using single DES with key K_1 . Then it will decrypt the output of step 1 using single DES with key K_2 . After that the output of step 2 is encrypted using single DES with Key K_3 . The final output of step 3 is the cipher text. The decryption is a vice versa reverse process. The user has to first decrypt the K_3 key and finally.

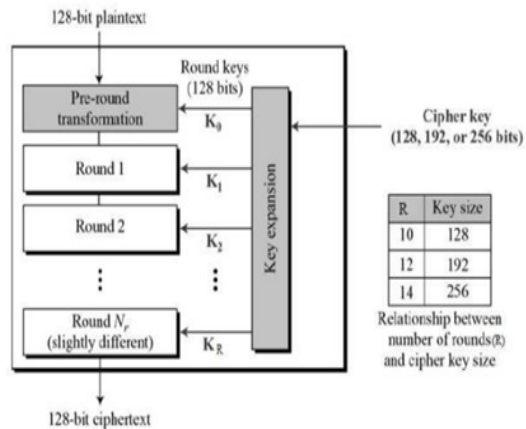


Figure 5.1 AES

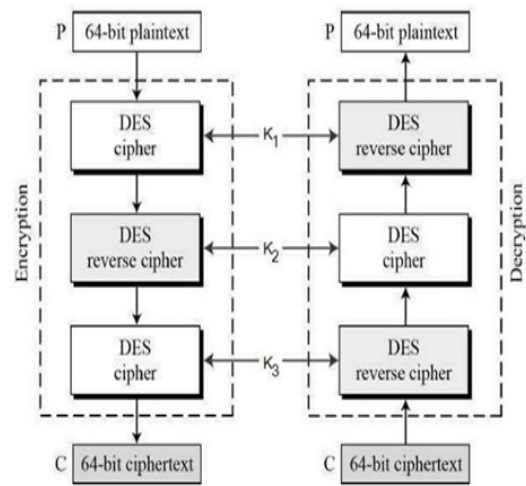
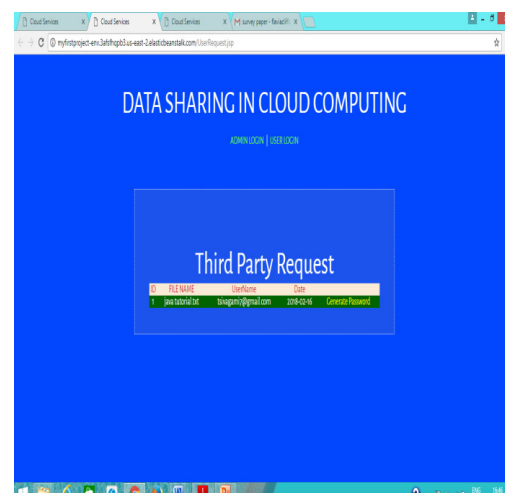
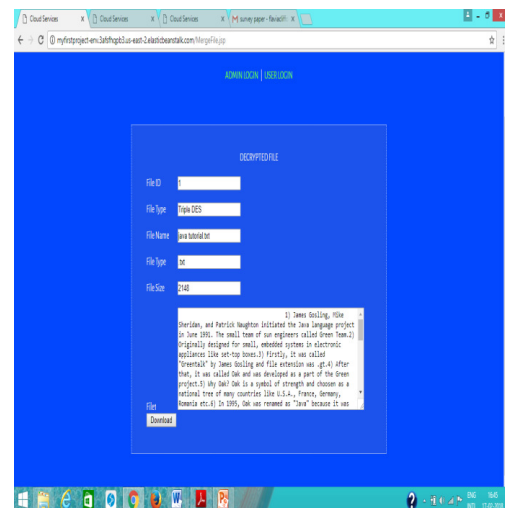
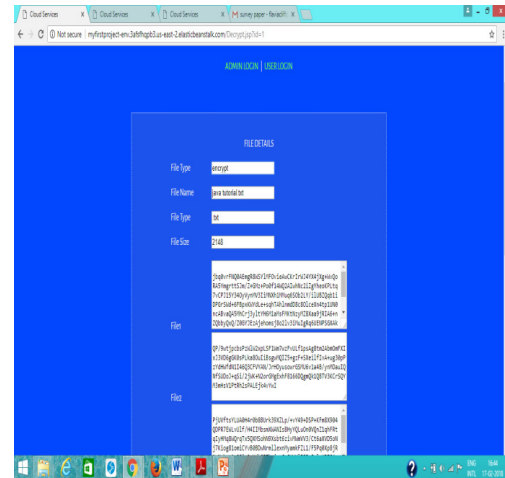


Figure 5.2 Triple DES

K1 key. Apart from these two a public key cryptographic algorithm asymmetric algorithm (RSA) is used. It will have two different keys, one of which can be given to anyone. That's why it's called public key. In this paper the user directs the public key to the server and demands for certain data. The server then encrypts the data using the user's public key and sends the encrypted data. While in the receiver end, the user obtains the data thus decrypts it. As, this is an asymmetric one part from the authorized entity can decrypt the information even if the third party has a public key.



6. Conclusion

The security and privacy of information that are stored CSP (Cloud Storage Providers) has significant prominence of challenges and of paramount prominence. Cryptographic techniques are used for protect vulnerable communications between users and the Cloud providers. Thus for enhancing the cloud security in network we use partition and encryption of information. This paper put forward a mix of Symmetric and Asymmetric encryption algorithm Symmetric encryption has computational competence and rapidity to handle large volumes of information from cloud storage providers that are demanded by the cloud users. By using this type of encryption algorithm, user confirms data is stored securely and it cannot be retrieved by CSP Administrators or intruders. Data integrity is taken care along with security constraint to achieve the finest conceivable results.

References

- [1] Chen, F., Xiang, T., Yang, Y. and Chow, S.S., 2016. Secure cloud storage meets with secure network coding. *IEEE Transactions on Computers*, 65(6), pp.1936-1948.
- [2] Wang, C., Chow, S.S., Wang, Q., Ren, K. and Lou, W., 2013. Privacy-preserving public auditing for secure cloud storage. *IEEE transactions on computers*, 62(2), pp.362-375.
- [3] Yang, M. and Yang, Y., 2010. A hypergraph approach to linear network coding in multicast networks. *IEEE Transactions on Parallel and Distributed Systems*, 21(7), pp.968-982.
- [4] Wang, boyang, Baochun Li, and Hui Li, 2015. "Panda: Public auditing for shared data with efficient user revocation in the cloud". *IEEE Transactions on service computing* 8.1(2015):92-106.
- [5] V.S. Mahalle, A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa&Aes) Encryption Algorithm", *IEEE INPAC*, pp. 146-149, Oct. 2014.
- [6] Abu Marjan, Palash Uddin, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography", *IEEE IFOST*, pp. 14-17, October 2014.
- [7] P. S. Bhendwade, R. T. Patil, "Steganographic Secure Data Communication", *IEEE International Conference on Communication and Signal Processing*, pp. 953-956, April 2014.
- [8] S.Hesham, Klaus Hofmann, "High Throughput Architecture for the Advanced Encryption Standard Algorithm", *IEEE International Symposium on Design and Diagnostics of Electronic Circuits & Systems*, pp. 167-170, April 2014.
- [9] M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput", *IEEE ICCCI*, pp. 1-5, January 2014.
- [10] Yingbing Zhou, Yongzhen LI, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", *IEEE ICSESS*, pp. 517-520, June 2014.
- [11] N. Sharma, A. Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", *IEEE International Conference on Reliability Optimization and Information Technology*, pp. 310-313, Feb 2014.
- [12] Singh Inder, M. Prateek, "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma A. Hasan "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", *IEEE International Conference on Reliability Optimization and Information Technology*, pp. 310-313, Feb 2014.
- [13] K. Jasleen, S. Garg, "Security in Cloud Computing using Hybrid of Algorithms", *IJERJS*, vol. 3, no. 5, pp. 300-305, September–October 2015, ISSN 2091-2730.
- [14] S. Munjall, S. Garg, "Enhancing Data Security and Storage in Cloud Computing Environment", *IJCSIT*, vol. 6, pp. 2623-2626, 2015, ISSN 0975-9646.
- [15] U. Veeresh, S.P. Kumar, "Multi Cloud Architecture to Provide Data Privacy and Integrity", *IJCERT*, vol. 2, no. 9, pp. 558-564, September 2015, ISSN 2349-7084.
- [16] M. Rajesh, Manikanthan, "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning", *International Journal of Pure and Applied Mathematics*, ISSN NO:1314-3395, Vol-116, No. 21, Oct 2017.
- [17] T. Padmapriya, V.Saminadan, "Performance Improvement in long term Evolution-advanced network using multiple input multiple output technique", *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 9, Sp-6, pp: 990-1010, 2017.

