Multilevel Encryption for Cloud Storage

Deepti Rai*, Roopa Desai, Tripti P S and Vinutha B

Department of Information Science and Engineering, Sahyadri College of Engineering & Management, Mangaluru – 575007
*Email: akhila.is@sahyadri.edu.in

ABSTRACT

InformationCloud storage has easy access anytime, anyplace, anyhow due to its scalability, cost efficiency, and high reliability of the data. Cloud computing uses internet for computing services. Organizations are moving their data to cloud. So we have to protect uploaded data against unauthorized users from data access, modification etc. In this paper, a multilevel encryption and decryption for cloud storage is proposed. Here a combination of AES and Rounded shift algorithm is used. Thus, only a valid user will access and modify the data file. If an intruder takes the confidential data intentionally or accidentally, one must have had to decrypt the data for at each level. So, there is less probability of getting original data. It is expected that using double level encryption and decryption will provide more security of cloud storage that using one level for encryption and decryption.

***Keywords:** Cryptograph, Security algorithm, AES, Rounded shift, Symmetric, Asymmetric*

1. INTRODUCTION

In this new era, Cloud computing provides large number of services of internet. For cloud services allows user to utilize software and hardware that will be managed by unauthorized or invalid users. Cloud services mainly used for file storage, webmail and business application. Security to the data that resides in the cloud is provided by cryptographic algorithms. By using cryptography original data called plain text is converted into non readable form called cipher text. Existing cryptographic algorithm uses single level encryption and decryption so cyber criminals can easily break single level encryption.

Hence we propose the system that consists of multilevel encryption and decryption to provide security to cloud data. In our proposed system we implement two algorithms in which first level of encryption is done by Advanced Encryption Standard (AES) and second level encryption is done by Rounded Shift algorithm which is of Caesar Cipher type. AES will process huge amount of data and that has high speed of performing encryption and decryption which is more secure. Caesar Cipher also known as shift cipher which consists of left and right shifts. Here each bit of plain text is shifted in Caesar box to a certain position using key. In our paper, we use modified Caesar cipher for better security purpose. When user uploads file it undergoes first level encryption using AES algorithm and here plain text is converted into cipher text. This scrambled form again undergoes second level encryption using Rounded Shift algorithm and these encrypted data stored in cloud database. When user wants to retrieve data from cloud decryption is done in the reverse order of encryption. Thus user gets the original data. In multilevel encryption it is difficult to guess the key for intruder.

Architecture design shows the conceptual model of the application. A graphical representation of concepts, their principles, elements and components that are part of architecture. The general architectural diagram of Multilevel Encryption/Decryption for Cloud Storage is shown in Figure. This design consists two level of encryption and decryption. Initially when user uploads the file, it undergoes first level of encryption using AES algorithm. During this original data is converted to cipher text and this cipher text undergoes second level of encryption using Rounded Shift algorithm. This encrypted data is stored in cloud database. When the user wants to download the file, the file is retrieved from cloud database and it undergoes two level of decryption using Rounded Shift and AES algorithm respectively. During each level of decryption cipher text is converted to plain text. Thus user gets original data file.

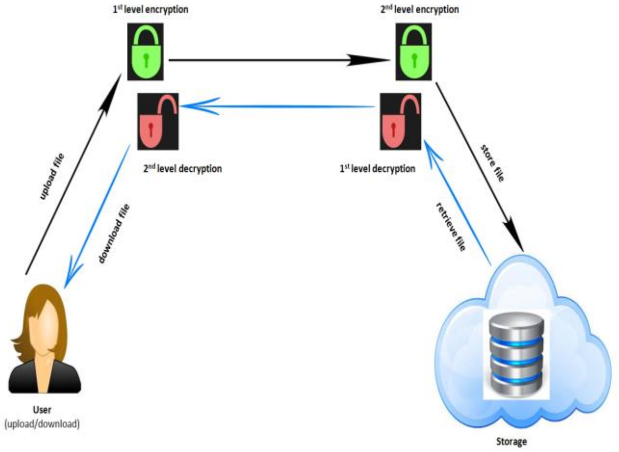

Figure 1: Architecture diagram of multilevel encryption / decryption for cloud storage

2. LITERATURE SURVEY

Data security in the cloud will be increased for using RSA and AES encryption and decryption algorithm. Here it uses key size of 1024 bit and 128 bit, so attacker cannot determine private key even if public keys are generated. The performance can be analysed with the help of file size and computation cost. This paper uses symmetric and asymmetric algorithm wherein asymmetric public of key is used by encryption to and private for key is for used by decryption. In symmetric one key is used for either an encryption or a decryption. Security can be enhanced using both symmetric and asymmetric algorithm. Hash and signature algorithms used to compress data [1]. The major issue related for cloud security of data integration. As a solution Byzantine for fault-tolerant protocol across over multiples of clouds is used. Another major concern is service availability. It prevents loss of customer private data as about result for malicious insiders out of clouds. This paper uses cloud computing of model includes of five characteristics features [2]. Security can be gained by applying cryptographic for methods by enclosing data decryption key only of the registered users. But here solution produces many computation times over the data owner on key distribution with management. This problem can be overcome by using attribute-based encryption like proxy decryption and lazy decryption. Data access control is developed by implementing fine grained to access by control, with leads to edibility of differential access with rights on individual users [5]. The system architectures used concatenating of digitalized signature algorithm of Diffie Hellman and AES as encryptions. Block tag form of authentication is used to maintain data over cloud storage. So there was need to remoting data integrity along provides security regards of user data. The combination with authentications techniques and key exchanged algorithms is implemented and that leads to three way of mechanisms. Here key distribution done in decentralized manner. Data slicing was doing through data for fragmentation technique to create segments of data. Datasets get slice onto three segments with using vertical, horizontal of mixed fragmentation with techniques. [6].

3. IMPLEMENTATION

Functional modules of multilevel encryption for cloud storage are:

1. Registration
2. Login into the system
3. Upload files
4. My files

3.1. Registration

Here new user signup into the system by entering username, mobile number, email, password which will be stored in the database for further reference.

3.2. Login into the system

Registered user can login into system for the upload, download and viewing the files which are stored in cloud.

3.3 Upload files

Here user chooses the file to be stored in the cloud. This file will undergo two level of encryption using rounded shift and AES algorithms before uploading it to cloud.

3.4. My files

Here get two options viz download and view. The file can be searched by its uploaded date and with file title. During download and view decryption is done in the reverse order of encryption and OTP is sent to the authorized user to access the file.

Here we are using two algorithms such as rounded shift algorithm and advanced encryption standard.

1) Rounded shift algorithm: Rounded Shift algorithm is Caesar-cipher type algorithm which uses the shifting of bits to encrypt the plain text. In this paper, we have used nine cross nine matrix which is further divided into nine blocks which is of three cross three matrix.

In first step this algorithm shifts fixed number of blocks as it defined in an algorithm. Later, in second step it shifts the bytes within the selected block based on the original length of the plain text. This generated cipher text is given as input to AES algorithm which is further encrypted using random generated keys. The decryption is done just by reverse order of encryption.

2) Advanced encryption standard (AES): Most popularized and with widely used symmetric of encryption algorithm is advanced encryption standard. AES is much faster than DES. The size of key used in DES is very small. It needed to be replaced by an algorithm. The feature with AES are symmetric of key, block cipher, 128 bit data, 128/192/256 bit keys. This algorithm treats the 128 bits in a plane text as a block of 16 bytes. The 16 bytes are arranged in the form of a matrix consisting of 4 rows and columns.

There are 4 steps in the encryption process.

1. Bytes substitution: Byte substitution is a step in which 16 bytes of input is substituted after looking up a fixed table which gives a matrix of 4 rows and columns.

2. Shifting of rows: Shifting of rows includes shift of the matrix's rows to the left, whichever entry which falls of re-inserted to the right of the row. The shifting is done randomly picking each row and shifting towards the left with random number of shifts. This step occurs in numerous number of times.

3. Mixing of columns: Mixing of columns is done by transforming each column which consists of 4 bytes using some mathematical function. This function replaces the original column of 4 bytes into completely new set of 4 bytes. This gives with result upon another unique in matrix which consists of 16 new with bytes.

4. Adding of round keys: Adding of round keys has 16 from bytes of matrix which are considered with 128 bits and is OR, forming a round key of same number of bits. This step is performed many number of times to get the output as cipher text. The decryption of cipher text is done by reversing the order of encryption process.

4. RESULTS AND ANALYSIS

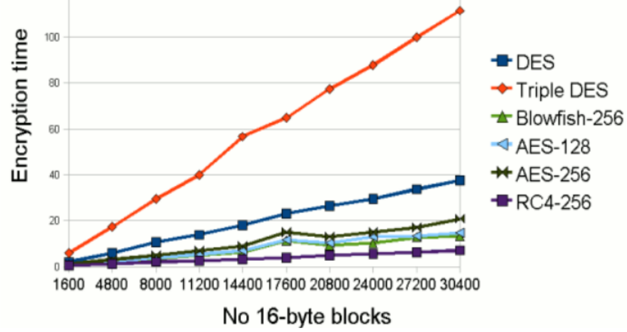

Fig. 2. Encryption speed of AES algorithm

Figure 2 shows the encryption speed of the algorithm. If the encryption speed is less then it gives better security. By using rounded shift algorithm it's difficult to predict encryption key. The above graph deals with the encryption time. It compares the AES algorithm with other encryption algorithms.

5. CONCLUSION AND FUTURE WORK

Multilevel Encryption for Cloud Storage provides security for the confidential data. The operations like upload, download and view are performed by registered user. Searching of file is provided with the help of file title and uploaded dates. It includes two levels of encryption by using Rounded shift algorithm which uses shift key for encryption. Here plain text is converted into cipher text of same length. Second level of encryption is done through AES algorithm which uses randomly generated key, it converts cipher text of rounded shift into 124 bit cipher text. Decryption is done in the reverse order of encryption. During view and download OTP is generated randomly and sent to the registered mobile number to authenticate whether valid user is logged in or not. Our proposed project support only for text and word file. So future enhancement can be encryption of images and pdf files.

REFERENCES

[1] Akashdeep Bharadwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry, "Security Algorithms for Cloud Computing", ELSEVIER, vol. 85, pp. 535-542, 2016.

[2] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System science, 2012.

[3] Eman M. Mohamed, Hatem S. Abdelkader, Sherif El-Etridy, "Enhanced Data Security Model for Cloud Computing", The 8th International conference on Informatics and systems, May 2014.

[4] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, pp. 109-116, 2009.

[5] Shucheng Yu, Cong Wang, Kui Ren, and Wenging Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", in Proc. of SP'02, 2009.

[6] Akhil Behl, Emerging Security Challenges in Cloud Computing, "An insight to cloud security challenges and their Mitigation", pp. 217-222, 2011.

[7] Mr. Rupesh R Bobde, Prof. Amit Khaparde, Prof. Dr. M. M. Raghuwanshi, "An Approach for Securing Data on Cloud Using Data Slicing and Cryptography", IEEE sponsored 9th international conference on intelligent system and control, 2015.