IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-9 E-ISSN: 2347-2693

An Approach to provide Secure Storage using Self Destructing Erasure Codes

B.Anusha[1*] and S.Phani Praveen[2]

[1*,2]Dept. of Computer Science and Engineering,
Prasad V Potluri Siddhartha Institute of Technology, Kanuru, India

www.ijcseonline.org

Received: Aug/27/2015 Revised: Sep/06/2015 Accepted: Sep/21/2015 Published: Sep/30/2015

***Abstract*—** Several encryption schemes provide data confidentiality but at the same time functionality of the storage system is limited. A threshold proxy re-encryption scheme which is integrated with decentralized erasure code was proposed to formulate a secure storage system. This scheme provides robust and secure storage and retrieval and also lets the user forward the data to other users. The main technical contribution is that encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted message are supported by this scheme.

***Keywords*—** proxy re-encryption, decentralized erasure code, RSA, AES, erasure codes

I. INTRODUCTION

Information security is the practice of defending information from unauthorized access, use, disruption, modification, inspection, recording or destruction. The act of ensuring that data is not lost when critical issues arise is called as Information assurance[1]. There is a serious concern for the confidentiality of data when it is stored in third party's system. There are schemes which provide confidentiality for data but with limited functionality. It is quite difficult to construct a system which provides several functions. Here mainly the focus is on constructing a system in which data is robust and the confidentiality of data is maintained. It also uses another method called Erasure Coding to represent a message of n symbols into a message of k symbols. By using these techniques encoding and storing process will be completed. Some of the cryptographic methods are used to provide better storage. At first the data is encoded and to get the original data then it is decoded. In our scheme the keys are distributed to independent servers and then the data is forwarded. By using the threshold proxy re-encryption scheme which is integrated with the decentralized erasure code and encryption is done by using RSA scheme. What exactly performed is at first the data is encrypted and forwarded and the encoded data is stored.

II. OVERVIEW

Security Concepts:

The basic security concepts are confidentiality, integrity and availability. It is also known as CIA triad is considered as the heart of information security[1]. Authentication, authorization and nonrepudiation are related to the people when information is used.

Confidentiality: When an unauthorized user tries to read the data then the confidentiality is lost[1]. The property of making information not made available to unauthorized user is called as confidentiality.

Integrity: When the data is changed unexpectedly then the integrity is lost[1]. Maintaining and assuring the accuracy and completeness of data over its entire life cycle is called Data Integrity[3].

Availability: When the data is removed or unable to access the data is said to be unavailable. The information must be available when it is needed[3].

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization[1]. Authentication is proving that a user is the person he or she claims to be. Authorization is the act of determining whether a particular user has the right to carry out a certain activity. When the authentication cannot be refuted it can say that security is strong and the user cannot later deny that he or she performed the activity. This is known as nonrepudiation[1][3].

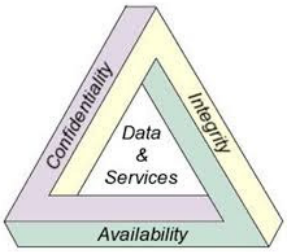


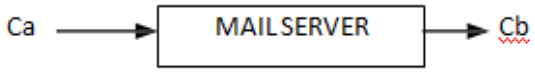
Figure 1: CIA Triad

Cryptography: It is the art of protecting information by transforming it into an unreadable format called cipher text. Only those who possess a secret key can decipher or decrypt the message into plaintext[7].

III. IMPLEMENTATION

a. Proxy Re-Encryption Scheme:

Proxy re-encryption is relatively a newly-devised cryptographic primitive[5]. The main aim of this scheme is to re-encrypt the cipher text firmly without depending on third parties[2].



By using a key b/a mod q the cipher texts are transferred from John to Smith. For better granularity improved proxy re-encryption scheme are used. Ateniese proposed Key-private proxy re-encryption scheme[5][6]. By using this key-private scheme a server cannot figure the uniqueness of the user. Pairing operations are done in most of the schemes but there are several other schemes in which pairing operations are not used[7]. Encoding operations over encrypted messages has been supported by this encryption scheme. Secret keys are shared to key servers with a break through limit t, by using a shamir secret sharing scheme[8]. To decrypt a message key server separately questions 2 servers. By using the moderately solved cipher texts k symbols can be obtained from the available key servers[6].

b. Decentralised Erasure Code:

It consider that n available servers have are k messages in the storage system. So that k messages can be retrieved by only querying any of the k storage servers. Storage servers are represented as (ss1, ss2,...), and key servers are represented as (ks1, ks2,...). Erasure coding is the technique of representing k sets of source data into n sets of data which is encoded in such a way that user can retrieve the original message from the encoded data[2]. Here k is nothing but the threshold limit. Each block is represented as a data item. On each data item arithmetic operations can be performed.

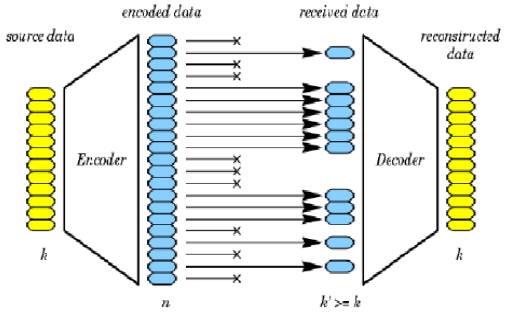


Figure 2: Representation of Erasure Coding

c. Cryptographic Scheme:

Here it uses a proxy re-encryption scheme and so use two different cryptographic schemes say RSA and AES[7]. For the generation of keys and for encrypting the data for the first time RSA is used. For re-encrypting the data AES is used[2].

A. RSA

Ron Rivest, Adi Shamir and Leonard Adleman proposed RSA algorithm. The RSA algorithm uses 2 different keys. Public key is used to encrypt the data and private key is used to decrypt the data. To encrypt the messages public key should be known. To decrypt the messages secret key must be known[4]. The working of RSA algorithm is as follows[8].

- Select two prime, say p and q.
- Calculate n = pq and z = (p-1)(q-1).
- Select a number, say e, e < n, which has no common factors (other than 1) with z.
- Find a number; say d, such that ed-1 is exactly divisible by z.
- Public key = (n, e), and Private key = (n, d).

Now the Encryption and Decryption of the algorithm is given as follows[8]:

Suppose John wants to send Smith a bit pattern, or number, say m such that m < n.

- To encrypt the message, John uses Smith's public key and determines the cipher text, say C as:
$$C = M^e \bmod n.$$
- To decrypt the message, Bob uses Bob's private key and determines the plain text, say M as:
$$M = C^d \bmod n.$$

B. AES

AES stands for Advanced Encryption Standard and it is a symmetric-key encryption standard. The ciphers has a block size of 128-bit and with the key sizes of 128, 192, 256 bits respectively[3].

High-Level Description of the Algorithm[3]:

These are the steps for AES

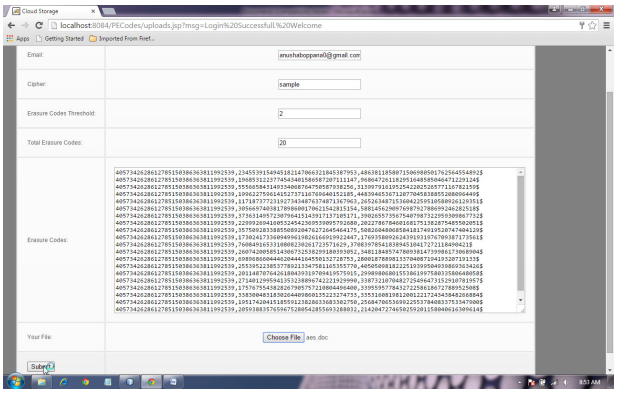
1) Key Expansion—Derive round keys from the cipher key.
2) Initial Round
   - Add Round Key – Using bitwise xor operation each byte of the state is combined with the round key.
3) Rounds

- Sub Byes – It is a non-linear substitution step where each byte is replaced with another by using a lookup table.
- Shift Rows – It is a transposition step where each row of the state is cyclically shifted towards the left.
- Mix Columns – A mixing operation is performed which operates on the columns of the state, combining the four bytes in each column.
- Add Round Key

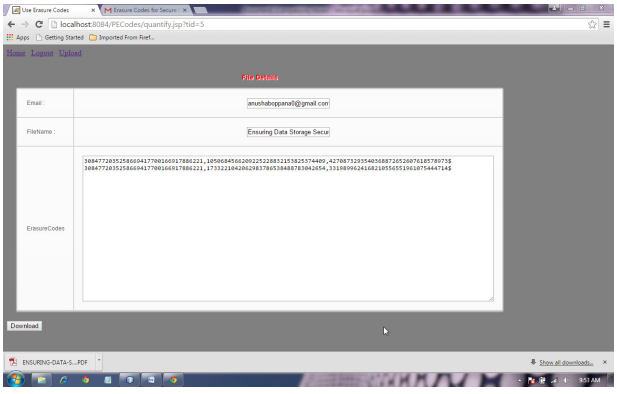
4) Final Round – There is no Mix Columns in this round.
   1. Sub Bytes
   2. Shift Rows
   3. Add Round Key

IV. RESULTS

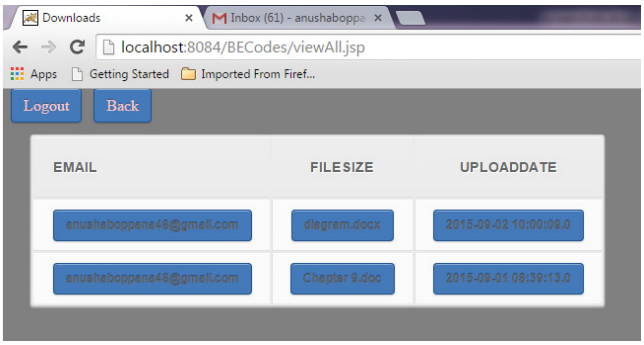
The user has to choose a file by providing the code word , Threshold limit and the no. of erasure codes and upload it by clicking on the submit button.



Once the user has downloaded the file by clicking on the "Save" button then that particular file will be downloaded and can be seen below in the browser window.



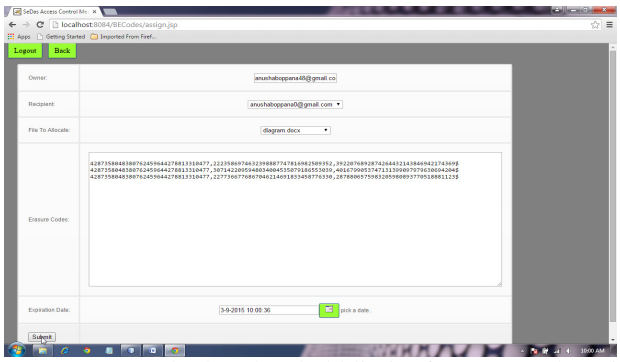
An authorized user can view all the files which were shared to him by other users who uploaded them and user can download the particular file user wants.



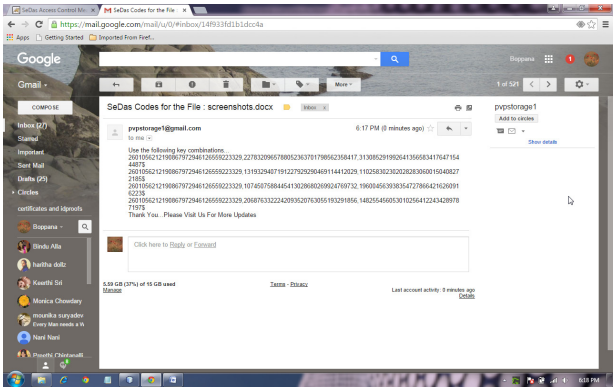
The user who has uploaded a file can share the files with other registered users of his interest. User has to choose a particular file and another user to whom user want to share that file. Here the threshold limit of the erasure codes will be automatically assigned and only the threshold no. of erasure codes will be sent to the registered mail-id of the user to whom the file was shared.

The main thing to be considered here was the user who is sharing a file with other users will share the erasure codes only for a particular time limit. The user sets expiration date and time for the erasure codes shared.

Once the keys have been expired then the user can't download the file by using those erasure codes.



Here only the Threshold limit of erasure codes will be sent to the registered mail-id the user to whom the keys were shared.



V. CONCLUSION

As storing and sharing our data securely is one of the difficult tasks today due to advancement in various fields. A Technique was proposed here for forwarding data securely in storage system. The blocks are divided and represented in encrypted and encoded format and saved in servers. For sending the data securely re-encryption is done and then stored in storage servers. When those blocks of data is to be retrieved the key servers performs decryption by using the re-encryption key. Thus encoding and decoding is done at storage servers and decryption is done by key servers. As this requires huge servers it needs to be implemented in real way for real results.

Future Work:

More ideas need to be implemented in this context to provide secure storage. Better algorithms with high performance results should be used for better results.

REFERENCES

[1] Introduction to Information Security, https://en.wikipedia.org/wiki/Information_security, Wednesday, July 1, 2015.

[2] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE.,‖ A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding‖, IEEE transactions on parallel and distributed systems, vol. 23, no.6, pp.995-1003 , june 2012.

[3] Rachna Jain, Sushila Madan and Bindu Garg, "Analyzing Various existing Security Techniques to Secure Data Access in Cloud Environment", Volume-3, Issue-1, January-2015.

[4] Evgeny Milanov ― The RSA Alorithm‖ 3 june, 2009.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ―Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,‖ ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

[6] G. Ateniese, K. Benson, and S. Hohenberger, ―Key-Private Proxy Re-Encryption,‖ Proc. Topics in Cryptology (CT-RSA), pp. 279-294, 2009.

[7] J. Shao and Z. Cao, ―CCA-Secure Proxy Re-Encryption without Pairings,‖ Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC), pp. 357-376, 2009.

[8] Shamir, ―How to Share a Secret,‖ ACM Comm., vol. 22, pp. 612-613, 1979

AUTHORS PROFILE

B.Anusha is presently M.Tech Student, Dept. of Computer Science & Engineering, Prasad V Potluri Siddhartha Institute of Technology (Autonomous), kanuru, A.P-India.

S.Phani Praveen is presently Assistant Professor, Dept. of Computer Science & Engineering, Prasad V Potluri Siddhartha Institute of Technology (Autonomous), kanuru, A.P- India.