International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Security of Discrete Data using Updatable Block-Level MLE, AES, and Steganography

Sneha Sukumaran N K, George T Vadakkumcheril

[1]*M.Tech student, Dept. of Computer Science and Engineering, IIET Nellikkuzhi*
[2]*Assistant Professor, Dept. of Computer Science and Engineering, IIET Nellikkuzhi*

Abstract – *The security of discrete media i.e texts and single images are mention in this project. Here we use combinations of two technology, i.e message locked encryption for text data and AES and triple DES for single image data. This paper initiates the study of updatable block-level MLE, a new primitive in incremental cryptography and cloud cryptography. Our proposed provably-secure construction is updatable with computation cost logarithmic in the file size. It naturally supports block-level deduplication. It also supports proof-of-ownership which protects storage providers from being abused as a free content distribution network. Our experiments show its practical performance relative to the original MLE and existing non-updatable block-level MLE. We used the steganography concept also.*

Key Words: **Message-Locked Encryption, Deduplication, Hash Function, AES Encryption, Steganography.**

1. INTRODUCTION

Now a day's the uses of devices like computer, mobile and many more other device for communication as well as for data storage and transmission has increases. Here arise data security problems. To overcome this uses the technology MLE, AES, Triple DES and Steganography. MLE provide deduplication, which eliminates redundant copies of user provided data, has been widely used to improve storage utilization and reduce communication cost. The saving is significant for (cloud) storage provider which stores data from many clients. The first attempt to resolve the seemingly contradicting requirements was convergent encryption [1]. Convergent encryption (and its variants) has been used in numerous applications [2]. However, the security guarantee is provided by convergent encryption is unknown until the formulation of message-locked encryption (MLE) [3]. MLE is a symmetric encryption scheme, in which the message is the lock, i.e., it uses the message to derive the key for encryption and decryption. While earlier MLE [3], focus on file-level deduplication, a study of practical deduplication [6] has shown that block-level deduplication can be more space-efficient. Naturally, recent research extended file-level deduplication on encrypted data to the block-level setting [5]. The most straightforward solution is to apply file-level MLE on each block independently.

1.1 OBJECTIVE

Data deduplication has been widely used in cloud storage to reduce storage space and communication problem by reduce same data and storing only one copy of them. Confidential and sensitive data stored in the cloud is extremely crucial. So that the main aim is to protect data sharing using keys.

1.2 SCOPE

The main scope of this is to provide security and reduce the storage space and avoid the communication problems of discrete data. The proposed mechanism is provide high security to the text data and the single image data.

2. RELATED WORK

All other works focus on static files, with no support of file update (even with the help of a key-management server). To modify a single bit, the file owner has to download the whole encrypted file, decrypt, update, re-encrypt, and then upload the new cipher text to the cloud. The computation and communication costs of all these operations are linear in the file size, which are too expensive for large files. In many applications, we need to incrementally update a large file that can be deduplicated across different users from time to time. An astronomers update high-resolution images of different parts of the universe periodical users may back up virtual machine images regularly.

3. PROPOSED SYSTEM

This project is implemented in a website model .the project use three technologies for the security of the discrete data i.e text and single image. The text files are uploaded using the updatable block-level message locked encryption the images uploaded by AES encryption and the steganography concept is also used.

The user can upload any type of data such as text or single images. The text data is encrypted using message locked encryption and the image data is encrypted by using the AES algorithm. The third concept is steganography. Here the steganography is used for the protection of the users password.

3.1 ENCRYPTION OF TEXT DATA

Encryption of text data is based on updatable block-level message locked encryption. The block-level MLE exists [5] and our definitions also extend for file-level MLE. MLE is a symmetric encryption technology. Here the message is the lock, i.e., it uses the message to derive the key for encryption and decryption. The MLE provide strong tag consistency, privacy, and context hiding. There are five algorithms are used parameter generation algorithm, key generation algorithm, encryption algorithm, tag generation algorithm, dec algorithm. All the other except the dec algorithm are probabilistic.

3.2 ENCRYPTION OF SINGLE IMAGE

Here we use AES encryption [4] technology for encrypt the single image and triple DES for decrypt the images in this way we can assure the security. For encryption purpose four rounds consist of substitute byte, shift row, six columns, add round key. AES specifies a federal information processing standards publication (FIPS) approved cryptographic algorithm that can be used to protect electronic data. Triple DES is the decryption technology used in this project. It is the reverse process of EDE encryption method. The user can use the same key for encryption and decryption. The sequential order is changes but the key remains the same.

Fig-1 (a) Original image (b) Encrypted image

3.3 STEGANOGRAPHY

Image steganography used to hiding the data such as text, image, audio files into another image. Here used this technique is to secured the user password. In this way we can prevent the hackers attack. The hidden information decoding through a proper decoding technique. Fig – 1 shows the working model of the steganography technology. There is no difference between the original file and the file with the message embedded into it. This is accomplished by storing the message using LSB (Least Significant Bits) in the data file.

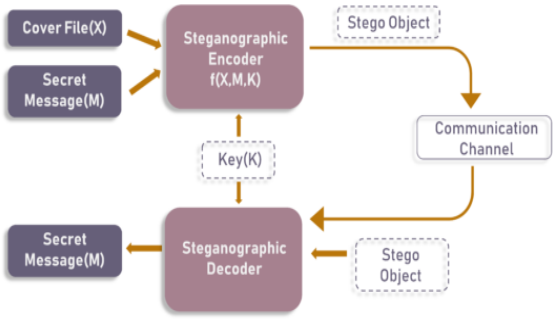

Fig - 1 working model of steganography

4 CONCLUSION

Here initiate the study of security of discrete data. I conclude that encryption does not preclude deduplication or efficient ciphertext updates. The proposed system allows insertions, updates, deletions of discrete data and it provides high security. A Successful implementation of symmetric key AES algorithm is one of the best encryption and decryption standard available in market. Including the steganography concept is providing high security also.

REFERENCES

[1] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system," in IEEE ICDCS, 2002.

[2] A. Adya, W. J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J. R. Douceur, J. Howell, J. R. Lorch, M. Theimer, and R. Wattenhofer, "FARSITE: federated, available, and reliable storage for an incompletely trusted environment," in OSDI, 2002.

[3] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in EUROCRYPT, 2013.

[4] An image encryption and decryption using AES algorithm-Priya Deshmukh.

[5] R. Chen, Y. Mu, G. Yang, and F. Guo, "BL-MLE: block-level message-locked encryption for secure large file deduplication," IEEE Trans. Information Forensics and Security, vol. 10, no. 12, 2015.

[6] D. T. Meyer and W. J. Bolosky, "A study of practical deduplication," TOS, vol. 7, no. 4, 2012.