International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 278-282, May-2023

https://doi.org/10.47001/IRJIET/2023.705037

Image and Text Encrypted Data with Authorized Deduplication in Cloud

[1]Shubham Borade, [2]Abdulrehman Khan, [3]Abdullah Khan, [4]Afridi Sayyed, [5]Prof. Ranjana M. Kedar

[1,2,3,4]Student, Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India

[5]Professor, Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India

***Abstract* - With the advent of cloud computing, secured data deduplication has gained a lot of popularity. Many techniques have been pro-posed in the literature of this ongoing research area. Among these techniques, the Message Locked Encryption (MLE) scheme is often mentioned. Researchers have introduced MLE based protocols which provide secured deduplication of data, where the data is generally in text form. As a result, multimedia data such as images and video, which are larger in size compared to text files, have not been given much attention. Applying secured data deduplication to such data files could significantly reduce the cost and space required for their storage .In this paper we present a secure deduplication scheme for near identical (NI) images using the Dual Integrity Convergent Encryption (DICE) protocol, which is a variant of the MLE based scheme. In the proposed scheme, an image is decomposed into blocks and the DICE protocol is applied on each block separately rather than on the entire image. As a result, the blocks that are common between two or more NI images are stored only once at the cloud. We provide detailed analyses on the theoretical, experimental and security aspects of the proposed scheme.**

Keywords: Cloud Computing, Data Deduplication, Message Locked Encryption, Dual Integrity Convergent Encryption (DICE), protocol.

I. INTRODUCTION

Cloud computing provides users with the platform to avail cloud services on demand which include primarily storage, database, networking, and software services over the Internet. Whether a user is watching movies, listening to audio, taking pictures, hosting websites or creating new apps, cloud computing is an integral part of all these services. Cloud service providers (CSPs) charge their users a nominal fee for the use of these services. Therefore, it is important for the CSPs to maintain a tradeoff between the cost of the services they provide and the fees that they charge to their users, as maintaining and storing the huge volume of users' data, along with the bandwidth usage incur costs for the CSPs. CSPs rely on deduplication techniques to remove duplicate data and thus reduce bandwidth and storage requirements. However, it is equally important for CSPs to ensure the privacy and security of users' data. To address both these issues, secured data deduplication was introduced, in which duplicate data is removed while maintaining the confidentiality of the users' data.

II. LITERATURE SURVEY

1) Paper Name: Secondary Encrypted Secure Transmission in Cognitive Radio Networks, Author: Dawei Wang; Pinyi Ren; Qian Xu; Qinghe Du

Abstract: In order to secure the primary privacy information and provide quality-of-service provisioning for the secondary system, we propose a secondary encryption secure transmission scheme. In the proposed scheme, the primary system utilizes the secure secondary messages to encrypt the primary confidential messages and the secondary system can acquire some spectrum opportunities. Specifically, when the primary system is secure, the primary information can be directly transmitted; when the primary system is insecure while the secondary messages can be securely trans-mitted, the primary system utilizes the secure secondary messages to encrypt the primary information; otherwise, the spectrum will be utilized for secondary trans-mission. For the proposed scheme, we investigate the performances of the primary ergodic secrecy rate and the average secondary throughput. Numerical results have demonstrated that the secondary encryption secure transmission scheme can secure the primary privacy messages and improve the secondary transmission throughput.

2) Paper Name: 3D-Playfair Encrypted Message Verification Technology based on MD5, Author: Wen-Chung Kuo; Wan-Hsuan Kao; Chun-Cheng Wang; Yu-Chih Huang.

Abstract: In the world of information development, the transmission of information is much more convenient. However, the transmission process always faces the risk of being attacked, stolen and tampered, which leads to the doubt that the data source is incorrect. For this reason, some scholars proposed to protect important information in the form of passwords. Alok et al. Proposed 3D-Playfair Cipher with Message Integrity using MD5. This paper uses 3D-Playfair

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 278-282, May-2023

https://doi.org/10.47001/IRJIET/2023.705037

encryption for encryption. However, simple 3D-playfair encryption cannot guarantee the integrity of data during transmission, so the author proposes Combined with MD5 to ensure the integrity of the data, but there are doubts about the credibility of the data source, so this paper uses XOR calculation methods to further verify the credibility of the data. When a man-in-the-middle attack is encountered, the attacker intercepts the packet and tampering with the data content can still accurately determine whether the source of the data is the original sender. This method guarantees the integrity of the data while improving the credibility of the data.

3) Paper Name: A Reversible Data Hiding Scheme in Encrypted Images by Con- trolled Pixel Modification, Author: K. Jagruth; V. M. Manikandan.

Abstract: Reversible data hiding is widely studied in recent years due to its wide applications in various domains such as medical image transmission and cloud computing. In this manuscript, we propose a novel scheme for performing reversible data hiding in encrypted images. In this scheme, the data hider can embed one-bit additional data bit in a small block (B × 2 pixels) from the encrypted image. All the non-overlapping regions (blocks) in the encrypted image will be processed by accessing those blocks in a predefined order. To embed a bit value 0 in an encrypted image block, no need to modify any pixel values. If we want to embed bit value 1, all the pixels in the first column of the selected image block will be mapped into a new pixel value based on a predefined function. At the receiver side, the data extraction and image recovery are carried by comparing the closeness between pixels in the adjacent columns of the pixels in each block of the decrypted image.

4) Paper Name: Dual Protection on Message Transmission based on Chinese Re- mainder Theorem and Rivest Cipher 4, Author: H. Kevin Ronaldo Cahyono; Christy Atika Sari; De Rosal Ignatius Moses Setiadi; Eko Hari Rachmawanto.

Abstract: This research proposes a combination of dual protection on text messages transmission using Chinese Remainder Theorem (CRT) steganography and Rivest Cipher 4 (RC4) encrypting method. This combination aims to optimize the performance of encryption and message insertion into an image. Security This message is done by encrypting text messages using RC4 first, then the results are embedded in the grayscale type container image with the CRT method. The evaluation standards that will be used in this research are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), and Character Error Rate (CER). MSE, PSNR and SSIM are used as a measure of the quality of stego images. To determine the performance ofthe proposed method, message insertion is carried out in three types of sizes, namely maximum payload, half payload and one quarter payload. While the CER is used to find out the results of decryption of text mes- sages. The resulting CER value is 0, this indicates the message was extracted and decrypted perfectly.

5) Paper Name: Image Steganography: 2-Bit XOR Algorithm Used in YCbCr Color Model with Crypto-algorithm, Author: Madhu D; S Vasuhi.

Abstract: Steganography is a study of invisible communication that typically ad- dresses how the message is concealed. Protection is required when we want to send data across any medium, this is why steganography has been built to safely send data in an image where the human eyes cannot identify it. This paper integrates cryptography and steganography through an image processing technique. YCbCr color model based on the 2-bit XOR LSB image steganography is proposed here in. The proposed scheme is a very safe technique for data concealed in the spatial field for image steganography, which converts an image from the color of RGB to the YCbCr space, and then secret data is concealed inside in the Cr color space compo- nent using 2-bit XOR.

III. METHODOLOGY

Secure data deduplication uses AES and MD5 algorithms. The AES algorithm is a symmetric block cipher algorithm that takes plaintext in blocks of 128 bits and transforms it into cipher text using keys of 128, 192, and 256 bits. The Advanced Encryption Standard (AES) is a specification for encrypting electronic data. AES is implemented in for de-duplication. The MD5 algorithm is the fastest algorithm. The proposed system uses Python because it facilitates text and image input system. In this we are using python tkinter module which is GUI (Graphical User Interface) library.

IV. PROPOSED SYSTEM

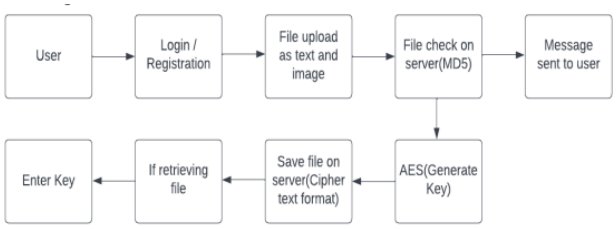

Figure 1: System Architecture

The proposed system uses the AES algorithm for encryption and decryption. AES is the most secure algorithm. The MD5 algorithm is used software and hardware around the world to encrypt sensitive data. The MD5 algorithm (Message Digest Algorithm) is most commonly used to check file integrity. The MD5 message-digest algorithm is cryptographically broken, but is widely used as a hash

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 278-282, May-2023

https://doi.org/10.47001/IRJIET/2023.705037

function that produces a 128-bit hash value. MD5 is a faster algorithm.

V. ALGORITHMS

A) AES Algorithm

A symmetric block cypher algorithm with a block/chunk size of 128 bits is the AES Encryption algorithm, also referred to as the Rijndael algorithm. These distinct blocks are converted using keys that are 128, 192, and 256 bits long. It then connects these blocks to create the cipher text after encrypting each one separately. Example:-It uses 256-bit encryption, which is regarded as being more sophisticated and secure. The one-to-one message is safely sent and received using 256-bit AES encryption on Facebook and WhatsApp.

Steps:

1. Byte substitution: In order to replace the 16 input bytes, a fixed table (S-box) provided in the design is looked up. A matrix with four rows and four columns rep- resents the outcome.

2. Shift rows: There are two ways to execute the shift row [4]. The fourth row is rotated three times if the parity is 1, and the second row is rotated by one [5]. The second row rotates by one and the third row by two if the parity is 0. Similar to how it happens during encryption, the rows of the state matrix are cycled through during decryption.

3. Mix columns: With the use of a static matrix, the MixColumns() function multiplies a specified ”state” matrix. The AES encryption mechanism makes use of the MixColumns() function. Using a static matrix and a provided “state,” the Mix- Columns() function multiplies the columns of the static matrix.

4. Add round key: Using the AES key schedule, KeyExpansion round keys are ob tained from the cypher key. For each round plus one, AES needs a distinct 128-bit round key block. Round one major addition: AddRoundKey - each byte of the state is combined with a byte of the round key using bitwise xor.

B) MD5 Algorithm

A string of any length can be hashed using the cryptographic hash method MD5 (Message Digest Method 5), which produces a 128-bit digest. The digests are shown as 32-bit hexadecimal values. This technique was created in 1991 by Ronald Rivest to enable the verification of digital signatures.

As a checksum, MD5 can be used to ensure data integrity and protect it from accidental corruption. It has been discovered that this historically popular cryptographic hash function has numerous serious flaws.

A high-end consumer graphics card can decrypt complex 8-character passwords en crypted by MD5 in 5 hours using brute force assaults. The findings were nearly instantaneous for straightforward passwords made up only of lowercase letters or numbers.

VI. RESULTS

The some of the result screenshots are as follows:

A) Home Page:

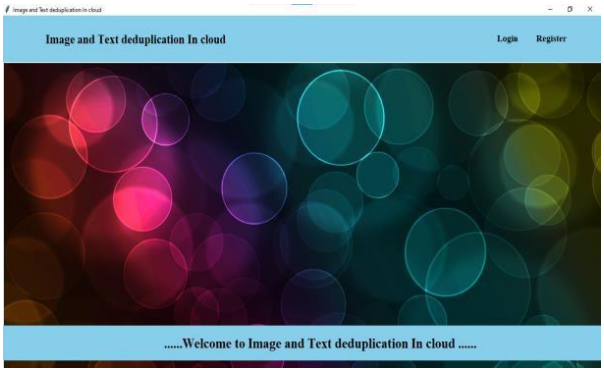

Figure 2: Home Page

B) Registration Page:

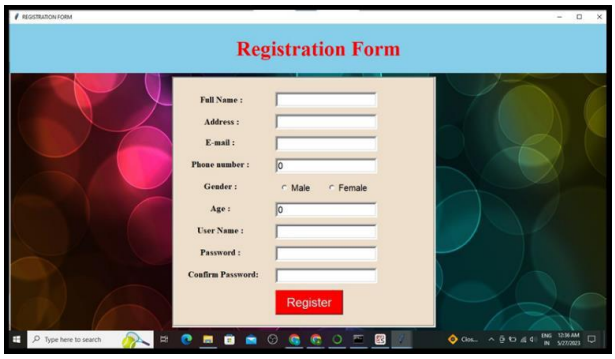

Figure 3: Registration Page

C) Login Page:

Figure 4: Login Page

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 278-282, May-2023

https://doi.org/10.47001/IRJIET/2023.705037

D) User Home Page:

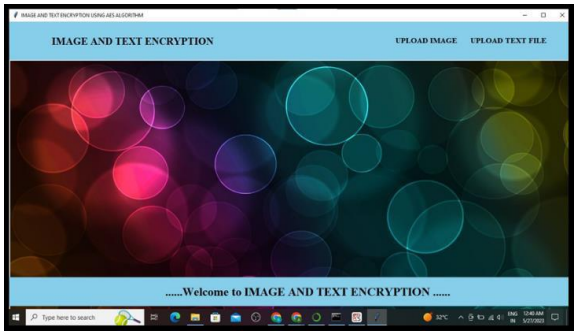

Figure 5: User Home Page

E) Encrypt Image:

Figure 6: Image Encryption Page

F) Decrypt Image:

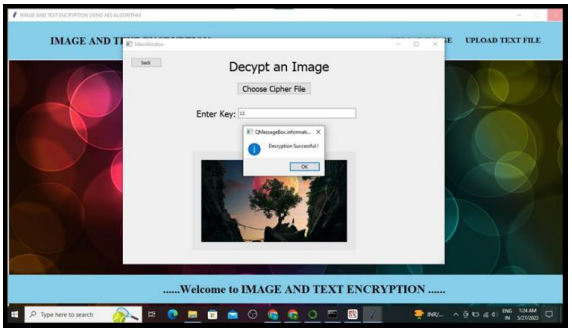

Figure 7: Image Decryption Page

G) Encrypt Text:

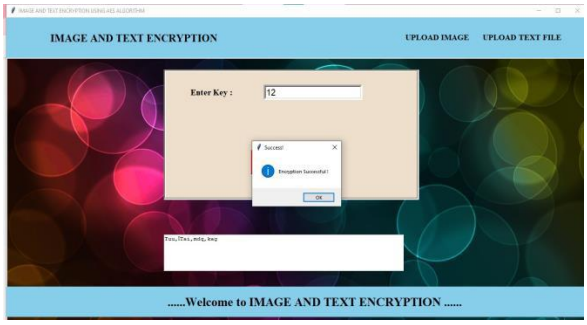

Figure 8: Text Encryption Page

H) Decrypt Text:

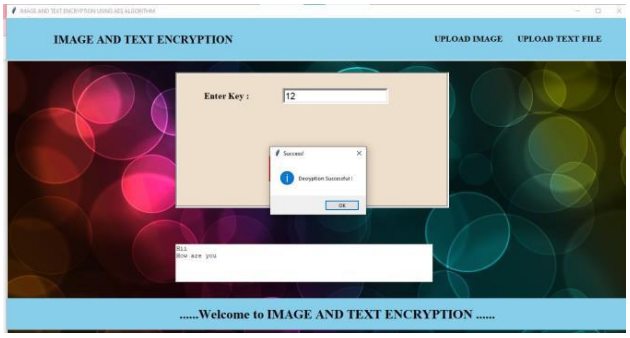

Figure 9: Text Decryption Page

VII. CONCLUSION

In this paper we discussed that to avoid the duplication using the Encryption and decryption method. And for the text uploading we are using three algorithms., For the uploading in the cloud system we are using the Structural Similarity AES Algorithm and the main purpose of the similarity index is to check the image quality such as luminance, contrast and structure, then it measures the similarity of two image. To store large amount of data with efficiency, to avoid the duplicate text and image we are using the encryption method. In this paper we have proposed Privacy preserving techniques for securing the PHI such as Layered model of access structure which solves the problem of multiple hierarchical files sharing. FH-CP-ABE is implemented which has low storage cost and computation complexity in terms of encryption and decryption. Deduplication is implemented which allows only a single instance of a file to be save which saves memory wastage and time. Odrive which connects all of the cloud servers together at the same time. In future work we will work towards designing a more secured system using AES (Advanced Encryption Standard (AES) which is stronger in detecting the attacks.

REFERENCES

[1] S. Halevi. D. Hornik. B. Pinkos. and A. Shulman-Peleg. “Proofs of ownership in remote storage systems,” in Proceedings of the 18th ACM SIGSAC Conference on Computer and Communications Security. ACM, 20 I I, pp. 491-500.

[2] Gonzalez-Manzano and A. Orfila., “An efficient confidentiality preselving proof of ownership for deduplication ,” Journal of Network and Computer Applications. vol. 50, pp. 49-59, 2015.

[3] J. Blasco, R. Di Pietro, A. Orfila, and A. Sorniotti. “A tunable proof of ownership scheme for deduplication using bloom filters,” in Comm1ications and Network Security (eNS). 2014 IEEE Conference on. IEEE.

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 278-282, May-2023
https://doi.org/10.47001/IRJIET/2023.705037

[4] W, K. Ng. Y. Wen, and H. Zhu, "Private data deduplication protocols in cloud storage," in Proceedings of the 27th Annual ACM Symposium on Applied Computinr; ACM, 20 12, pp. 441-446.

[5] R. Oi Pietro and A. Sorniotti. "Boosting efficiency and security in proof of ownership for deduplication." in Proceedings of the 7th ACM Symposium on Information. Computer and Communications Security. ACM, 20 12, pp. 81-82.

[6] M. Li. C. Qin, and P. P, C. Lee, "Cdstore; toward reliable, secure. and cost- efficient cloud storage via convergent dispersal," in Usenix Technical Conference, 20 15, pp. 45-53.

[7] Xu, E.-C. Chang, and l. Zhou, "Weak leakage-resilient client-side deduplication of encrypted data in cloud storage," in Proceedings of the Sd! ACM- SIGSAC symposiwn on Information, computer and communications security. ACM. 20 J3, pp. 195-206.

[8] "Private Data Deduplication Protocols in Cloud Storage" Wee Keong Ng SCE, Yonggang Wen SCE, Huafei Zhu.

[9] "DupLESS: Server-Aided Encryption for Deduplicated Storage" Mihir Bellare and Sriram Keelveedhi, University of California, San Diego; Thomas Ris-tenpart, University of Wisconsin—Madison.

[10] "RevDedup: A Reverse Deduplication Storage System Optimized for Reads to Latest Backups" Chun-Ho Ng and Patrick P. C. Lee The Chinese University of Hong Kong, Hong Kong Technical Report June 28, 2013.

[11] "A secure data deduplication scheme for cloud storage" Jan Stanek Alessan- dro Sorniotti, Elli Andreoulaki, Lukas Kencl.

[12] "Dynamic Data Deduplication in Cloud Storage" Waraporn Leesakul, Paul Townend, Jie Xu School of Computing University of Leeds, Leeds, LS2 9JT United Kingdom.

[13] "Side channels in cloud services, the case of deduplication in cloud stor- age" Danny Harnik IBM Haifa Research Lab Benny Pinkas Bar Ilan Univesity Alexandra Shulman-Peleg IBM Haifa Research Lab.

[14] "Memory Deduplication as a Threat to the Guest OS" Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, Cyrille Artho National Institute of Advanced Industrial Science and Technology.

AUTHORS BIOGRAPHY

Shubham Borade, Student, Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India.

Abdulrehman Khan, Student, Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India.

Abdullah Khan, Student, Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India.

Afridi Sayyed, Student, Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India.

Citation of this Article:

Shubham Borade, Abdulrehman Khan, Abdullah Khan, Afridi Sayyed, Prof. Ranjana M. Kedar, "Image and Text Encrypted Data with Authorized Deduplication in Cloud" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 5, pp 278-282, May 2023. https://doi.org/10.47001/IRJIET/2023.705037

****

