IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

Survey on Image and Text Encrypted Data with Authorized Deduplication in Cloud

Sneha Solepatil[1], Snehal Divekar[2], Akanksha Nagare[3], Digvijay Gaikwad[4], Prof. M. S. Kale[5]
Students, Department of Information Technology[1,2,3,4]
Professor, Department of Information Technology[5]
Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract: *Summaries are short summaries or abbreviated versions of the entire project, where we use machine learning techniques and algorithms to implement them. Cloud computing is a web-based computer system that is a large platform storage area that authorized users can access anytime and anywhere with a good internet or network connection. Cloud computing primarily provides shared resources and delivers hardware and software applications to devices on demand. It is like a remote server on the internet, which can store, manage and process data without using a computer. Therefore, the working time is faster compared to other local computers. Cloud computing is an information technology service and product. It supports virtualized resources based on IT infrastructure reusability. Cloud computing is the sequence of all required hardware, software, platforms, applications, infrastructure and storage with an online identity only. We use AES and MD5 algorithms for encryption and decryption after image and text encryption, then generate numbers and enter key to send emails.*

Keywords: Machine Learning, AES, MD5,Proxy re-encryption, Role authorized tree, Approved deduplication, Privacy leakage

I. INTRODUCTION

Cloud Computing is a web-based computer system, which is a large area of storage space, and authorized users can access the platform at anytime and anywhere with a good internet or network connection. Cloud computing mainly provides shared resources, hardware, software applications and other equipment on demand. It is like a remote server on the internet, which can store, manage and process data without using a computer. Therefore, the working time is faster compared to other local computers Cloud computing is an information technology service and product. It supports virtualized resources based on IT infrastructure reusability. Cloud computing is the sequence of all required hardware, software, software, platforms, applications, infrastructure and storage with an online identity only. It is the software and application-based platform used to access and also to manage the data storage with the help of network connectivity. The characteristics of cloud computing are on-demand self-service, measured service, rapid elasticity, resource pooling, broad network access.

II. LITERATURE SURVEY

1. Secondary Encrypted Secure Transmission in Cognitive Radio Networks

In order to protect the primary privacy information and provide high-quality. Service for the secondary system, we provide a secondary encrypted secure transmission scheme. In proposed scheme, the primary system encrypts the primary secrete message using a secure secondary message and the secondary system can obtained some spectrum opportunities. More precisely, when the primary system is secure, the primary information can be transmitted directly; when the primary system is not secure and the secondary message can be transmitted securely, primary system uses the secure secondary message to encrypt the primary information; otherwise, the spectrum will be used for secondary transmission. For the proposed scheme, we study the performance of the primary ergodic secrete rate and the average secondary through output. The numerical results show that the secondary encryption secure transmission scheme can protect the primary private message and improve the throughput of the secondary transmission.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

2. 3D-Playfair encrypted message verification technology based onof MD5

However, during the transmission process, there are always risks of attack, theft and tampering, which raise doubts about incorrect data sources. For this reason, some researchers suggest protecting important information in the form of passwords. Alok et al.3D-playfair encryption proposal with message integrity using MD5. This item uses 3D-playfair encryption algorithm for encryption. However simple playfair-3D encryption cannot guarantee the integrity of data during transmission, so the author suggests combining MD5 to ensure data integrity, but there are doubts about the credibility of the source of data, so this article adopts the XOR calculation method to further check the credibility of the data. When encountering man-in-the-middle attack, the attacker intercepts the data packets and the tempers with the data conte t and can still accurately determine whether the data source is the original sender. This method ensures the integrity of the data, while improving the credibility of the data.

3. A Reversible Data Hiding Scheme in Encrypted Images Modified by Control Pixel

Reversible data hiding has been widely studied in recent years due to its wide applications in various fields such as medical image transmission and cloud computing. In this manuscript, we proposed a new scheme to perform reversible data hiding in encrypted images. In this scheme, the data cache can hold an addition with bits of data from the encrypted image in a small box(B x 2 pixels). All non-overlapping regions(blocks) in the encrypted image will be processed by visiting there blocks in a predetermined order. Including a bit value of 0 in an encrypted image block does not require changing the pixel values. If we want to include a bit value of 1, all pixels in the first column of the selected image block will be mapped to new pixel values according to a predefined function. At the receiving end, data extraction and image restoration performed by comparing the proximity between pixels in adjacent columns of pixels in each block of the decoded image.

4. Double protection of message transmission based on Chinese remainder theorem and Rivest cipher

A combination of Chinese Remainder Theorem(CRT) steganography and Rivest Cipher 4(RC4) encryption method for double protection of text message transmission. This combination is designed to optimised encryption and message embedding performance in images. Security this message first encrypts the text message using TC4 and then embeds the result into a grayscale type container image using the CRT method. The endpoints that will be used in this stud are Mean Squared Error(MSE), Maximum signal to Noise Ratio(PSNR), Structural Similarity Index(SSIM), and Character Error Rate(CER). MSE, PSNR and SSIM are used to measure the quality of steganographic images. To determine the performance of the proposed method, message insertion is performed with three types of sizes, namely maximum pay load, half payload and quarter payload and CER is used to know the decryption result of SMS. The resulting CER value is 0, indicating that the message was successfully extracted and decrypted.

5. Paper name: Image Steganography

2bit XOR algorithm used in YCbCr colour model with Cryptographic algorithm.

Steganography is the study of invisible communication, usually involving how to hide messages. Protection is needed when we want the want to send the data over any media, that is why steganography is designed to data securely in images that are unrecognisable to the human eye. This article combines cryptography and steganography through image processing techniques. Here, YCbCr colour model based on 2bit LSB XOR image steganography is proposed.The scheme proposed in a very secure data masking technique for the spatial field of image steganography, which converts the image from RGB colour to YCbCr colour space and then secretes the data to Cr colour space. Using the hidden 2bit XOR component.Shachi Mall et al. [9],Xu Wu et al.[10], N. Shelke et. al. [11] and S. L. Bangare et. al. [12-14], V. Durga Prasad Jasti et. al. [15] have shown different methods for machine learning.

III. PROPOSED SYSTEM

In the recommendation system, we use the AES method for encryption and decryption, as well as data protection and security access control. MD5 technology should be used to avoid data duplication. The main overview of the proposed work is to avoid the duplication in the cloud server. We are avoiding the text duplication with the help of three

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

algorithms and role re-encryption. Before, in existing system they just avoided the text duplication with the help of two encryption algorithm. They are convergent encryption and role re-encryption.

IV. SYSTEM ARCHITECTURE

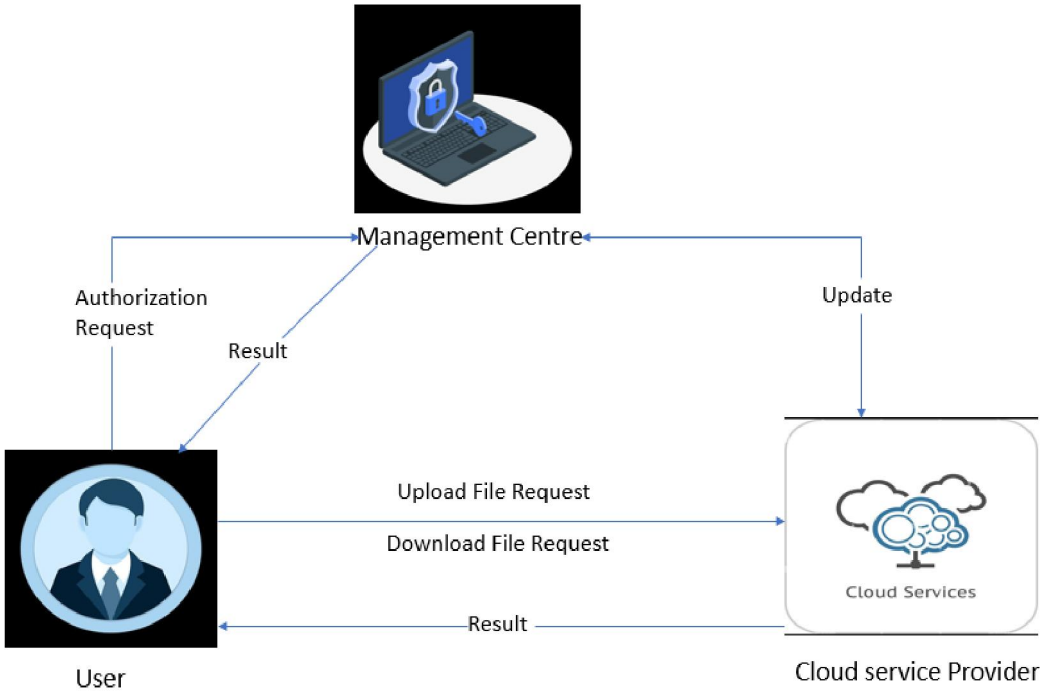

Fig.1. System Architecture

A user sends a request to Management centre, and encrypts the file, then it results as the cipher text to CSP. Users who belong to completely different role groups owning the corresponding role keys, with the role keys the user access cloud server, the user will upload or transfer the files from Cloud Service Provider. And user can download the file from the cloud server. A Cloud Service Provider is mainly for data storage, management and verification. Cloud Service Provider stores and manages the uploaded files from authorized users. Management centre is the trusted third party that is for the authorized user and for the role key management.

V. ALGORITHM

5.1 AES - Encryption Decryption Algorithm

The AES encryption algorithm is a symmetric block cipher with a block size of 128 bits. It transforms these individuals block using 128, 192 and 256-bit keys. Once it has encrypted the blocks, it concatenates them to form the cipher text. Advanced Encryption Standard (AES) is a symmetric clock code developed in the United States. The government protects classified information. AES is implemented in software and hardware around the world to encrypt sensitive data. It is essential to government computer security, network security and electronic data protection.

5.2 MD 5 - Data Deduplication

Methodology: MD5: The MD5 message digest algorithm is a cryptographically broken but still commonly used hash function that produces a 128-bit hash value. The MD5 hash function was originally designed as a secure cryptographic hashing algorithm for verifying digital signatures. But MD5 has been decrypted for users other than as a non-cryptographic checksum verify a data integrity and detect unintentional data corruption.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

VI. FUTURE SCOPE

- In future, we will try to use another encryption and decryption technique, such as Triple DES.
- RSA, Puffer Fish, Fishes.
- In future, we can use multiple ciphers.

VII. CONCLUSION

In this article, we have discussed avoiding duplication by using encryption methods. And to download text, we use three download algorithms in the cloud system, we use the structure similarity algorithm, the main purpose of the similarity index is to check text image equality, such as brightness, contrast, structure and then measure the similarity of the image. Two pictures in order to efficiently store large amount of data and to avoid respective text and image, we use encryption methods.

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 confidentialitypreserving 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. "An unable proof of ownership scheme for deduplication using bloom filters," in Comm\U1ications and Network Security (eNS). 2014 IEEE Conference on. IEEE.

[4]. J. Xiong, J. Ren. L. Chen et al.. "Enhancing privacy and availability for data clustering in intelligent electrical service of iot," IEEE Internet of Things Journal. vol. 6, no. 2, pp. 1530- 1540,April 2019.

[5]. Y. Zhang, X. Chen, l. Li. D. S. Wong, H. Li, and I. YOll, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," Information Sciences, vol. 379. PI>. 42-61,2017.

[6]. N.i, K. Zhang, Y. Yu et aI., "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," IEEE Trans. on Dependable and Secure Computing, vol. PP,no. 99,pp. 1-1,2018.

[7]. Liu, N. Asokan, and B. Piokas, "Secure deduplication of encrypted data without additional independent servers," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 20 IS, pp. 874-885.

[8]. l. Li, Y. K. Li, X. Chen, P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5. pp. 1206-1216, May 2015.

[9]. Shachi Mall, Ashutosh Srivastava, Bireshwar Dass Mazumdar, Manmohan Mishra, Sunil L. Bangare, A. Deepak, "Implementation of machine learning techniques for disease diagnosis", Materials Today: Proceedings, Volume 51, Part 8, 2022, Pages 2198-2201, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.11.274.

[10]. Xu Wu, Dezhi Wei, Bharati P. Vasgi, Ahmed Kareem Oleiwi, Sunil L. Bangare, Evans Asenso, "Research on Network Security Situational Awareness Based on Crawler Algorithm", Security and Communication Networks, vol. 2022, Article ID 3639174, 9 pages, 2022. https://doi.org/10.1155/2022/3639174

[11]. N. Shelke, S. Chaudhury, S. Chakrabarti, S. L. Bangare et al. "An efficient way of text-based emotion analysis from social media using LRA-DNN", Neuroscience Informatics, Volume 2, Issue 3, September 2022, 100048, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2022.100048

[12]. S. L. Bangare, G. Pradeepini and S. T. Patil, "Brain tumor classification using mixed method approach," 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070748

[13]. S. L. Bangare, G. Pradeepini, S. T. Patil, "Implementation for brain tumor detection and three dimensional visualization model development for reconstruction", ARPN Journal of Engineering and Applied Sciences (ARPN JEAS), Vol.13, Issue.2, ISSN 1819-6608, pp.467-473. 20/1/2018

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

http://www.arpnjournals.org/jeas/research_papers/rp_2018/jeas_0118_6691.pdf

[14]. S. L. Bangare, "Classification of optimal brain tissue using dynamic region growing and fuzzy min-max neural network in brain magnetic resonance images", Neuroscience Informatics, Volume 2, Issue 3, September 2022, 100019, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2021.100019

[15]. V. Durga Prasad Jasti, Enagandula Prasad, Manish Sawale, ShivlalMewada, Manoj L. Bangare, Pushpa M. Bangare, Sunil L. Bangare, F. Sammy, "Image Processing and Machine Learning-Based Classification and Detection of Liver Tumor", BioMed Research International, vol. 2022, Article ID 3398156, 7 pages, 2022. https://doi.org/10.1155/2022/3398156