JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Image And Text Encrypted With Authorized Deduplication In Cloud

Anish Karkhanis, Pratik Bhor, Priti Ugale, Sakshi Bhongale

Ms. Jaitee A. Bankar, Assistant Professor, IT Department, RMDSSOE, Pune
RMD Sinhgad School oF Engineering Warje ,Pune India

Abstract-*. In Cloud Storage, the role re-encryption is used to avoid the privacy data leakage and also to avoid the deduplication in a secure role re- encryption system(SRRS). And also it checks for the proof of owner- ship for to identify whether the user is authorized user or not. This is for the efficiency. Role re-encryption method is to share the access key for the corresponding authorized user for accessing the particular file without the leakage of privacy data. In our project we are using both the avoidance of text and digital images. For example we have the personal images in our mobile, handheld devices, and in the desktop etc., So, as these images have to keep secure and so we are using the encryption for to increase the high security. The text file also important for the users now-adays. It has to keep secure in a cloud server. Digital images have to be protected over the communication, however generally personal identification details like copies of pan card, Passport, ATM, etc., to store on one's own pc. So, we are protecting the text file and image data for avoiding the duplication in our proposed system.*

Index Terms- Searchable Encryption, Deduplication, Proof of Ownership, Proof of Storage.

I. INTRODUCTION

With the emergence of cloud storage service, managing business/personal data via a cloud storage provider such as Dropbox, OneDrive and Google Drive has become a common option. Affordable expense, high capacity, and more convenient service including data storage, access, and modification via the cloud anytime and anywhere make cloud storage a more appealing alternative over the conventional storage model. The statistics portal website statistics [1] forecasts that the number of personal cloud storage consumers will reach an estimated 2.3 billion worldwide by 2020. However, users' sundry uploads may overwhelm cloud service providers for the redundancy or duplicated documents will be amplified by the huge scale of the number of users.

Suppose that an international corporation deploys an enterprise-scale cloud architecture for sharing and storing corporate documents or operational data, then a large number of duplicated documents could exist in the storage. For instance, the leaders of the corporation release a document of regulation, all employees will download, learn and then store it under their own accounts. The trivial strategy is each file is stored once per account, resulting in a huge waste of storage resource. Message-locked encryption was hence proposed [2] to reduce redundancy, where the encryption key is derived from the message so the same message leads to the same key and ciphertext. MLE may face data privacy threats from various attackers including the cloud server and clients.

Text and Image data It has to keep secure in a cloud server. Digital images have to be protected over the communication, however generally personal identification details like copies of pan card, Passport, ATM, etc., to store on one's own pc. So, we are protecting the text file and image data for avoiding the duplication in our proposed system.

Compared with target-based deduplication, source based deduplication needs a client not to re-upload a document but merely a tag if there is already a duplicated one in storage, thereby advantageous in communication cost. However, source-based deduplication is subject to owner impersonating attacks where a validate tag is forged based on eavesdropped partial information. Such attacks spawned the notion of Proof of Ownership (POW) [4] where the client needs to prove to the server the possession of the whole file.

II. OVERVIEW

Text and Image data It has to keep secure in a cloud server. Digital images have to be protected over the communication, however generally personal identification details like copies of pan card, Passport, ATM, etc., to store on one's own pc. So, we

are protecting the text file and image data for avoiding the duplication in our proposed system.
emergence of cloud storage service, managing business/personal data via a cloud storage provider such as Dropbox, OneDrive and Google Drive has become a common option.
To construct a system with all mentioned merits, a trivial solution is to simply combine all existing techniques. For instance, the leaders of the corporation release a document of regulation, all employees will download, learn and then
store it under their own accounts. If cloud service providers choose one of these schemes as the core technique of the cloud system, additional independent modules must be deployed simultaneously in orderto obtain functionalities unrealized by the scheme. Then besides the significant increase on the storage, computation and communication cost, extra adjustment is needed for letting all modules collaborate as a whole.All interfaces and parameters should be correctly docked and all parameters adjusted.

III .OBJECTIVE

Encryption leverages advanced algorithms to encode the data making it meaningless to any user who does not have the key Authorized users leverage the key to decode the data transforming the concealed information back into a readable format. Then besides the significant increase on the storage, computation and communication cost, extra adjustment is needed for letting all modules collaborate as a whole. All interfaces and parameters should be correctly docked and all parameters should be well adjusted.

IV. LITRATURE SURVEY

[1] In this Paper **"**Secondary Encrypted Secure Transmission in Cognitive Radio Net-works" The Authors have Proposed Dawei Wang; Pinyi Ren; Qian Xu; Qinghe Du 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; whenthe 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 securethe primary privacy messages and improve the secondary transmission throughput.

[2] In this paper "3D-Playfair Encrypted Message Verification Technology " The authors Wen-Chung Kuo; Wan-Hsuan Kao; Chun-Cheng Wang; Yu-Chih Huang have proposed that **,**In the world of information development, the transmission of informa tion 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 Cipherwith Message Integrity using MD5. This paper uses 3D-Playfair 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 thedata. 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] In this paper "3D-Playfair Encrypted Message Verification Technology "
The authors Wen-Chung Kuo; Wan-Hsuan Kao; Chun-Cheng Wang; Yu-Chih Huang have proposed that **,**In the world of information development, the transmission of informa tion 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 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 thedata. 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.

[4] In this paper "Dual Protection on Message Transmission based on Chinese Remainder Theorem and Rivest Cipher 4"The Authors Kevin Ronaldo Cahyono; Christy Atika Sari; De Rosal Ignatius Moses Setiadi; Eko Hari Rachmawanto Have Proposed that 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 NoiseRatio (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 of the proposed method, message insertion is carriedout in three types of sizes, namely maximum payload, half payload and one quarterpayload. While the CER is used to find out the results of decryption of text messages. The resulting CER value is 0, this indicates the message was extracted and decrypted perfectly.

V. 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 algorithm., 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 .

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 presolving proof of ownersh ip 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 Comm1icationsand Network Security (eNS). 2014 IEEE Conference on. IEEE.

[4] W, K. Ng. Y. Wen, and H. Zhu, ”Private data deduplication protocols in cloud storage,” in Proceeding of the 27th Annual ACM Symposium on Applied Computing; 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] L. 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