International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 08, August 2017
ISSN: 2455-3778
http://www.ijmtst.com

A Privacy Preserving on Secure AES and Content Based Image Retrieval Scheme in Cloud Computing

L.Yazhini[1] | Dr.S.Santhosh Kumar S[2]

[1]M.Phil Scholar in Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.
[2]Professor, Department of Computer Science, Alagappa University, Karaikudi, Tamilnadu, India.

To Cite this Article
L.Yazhini and Dr.S.Santhosh Kumar S, "A Privacy Preserving on Secure AES and Content Based Image Retrieval Scheme in Cloud Computing", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 08, July2017, pp.-55-58.

ABSTRACT

In this paper we propose a secure framework for outsourced privacy-preserving storage and retrieval in large image repositories. Our proposal is based on a novel cryptographic scheme, named IES-CBIR, specifically designed for media image data. Our solution enables both encrypted storage and querying using Content Based Image Retrieval (CBIR) while preserving privacy. Our results show that IES-CBIR is provably secure, allows more efficient operations than existing proposals, both in terms of time and space complexity, and enables more realistic, interesting and practical application scenarios.

Keywords: *Searchable encryption, content-based image retrieval, secure AES, copy deterrence, watermark.*

I. INTRODUCTION

With the development of the imaging devices, such as digital cameras, smartphones, and medical imaging equipment's, our world has been witnessing a tremendous growth in quantity, availability, and importance of images. The needs of efficient image storage and retrieval services are reinforced by the increase of large-scale image databases among all kinds of areas. Meanwhile, after more than twenty years of development, CBIR techniques show the potential of usefulness in many real-word applications. For example, clinicians can use CBIR to find similar cases of patients and facilitate clinical decision-making processes. Large image database usually consists of millions of images. Therefore, CBIR services typically incur high storage and computation complexities. Cloud computing offers a great opportunity for the on-demand access to ample computation and storage resources, which makes it an attractive choice for the image storage and CBIR outsourcing. By outsourcing CBIR services to the cloud server, the data owner is relieved from maintaining local image database and interacting with database users online. Despite the tremendous benefits, image privacy becomes the main concern with CBIR outsourcing. For example, patients may not want to disclose their medical images to any others except to a specific doctor in medical CBIR applications. To formulate the problem, this paper considers two types of privacy threats. Firstly, a curious cloud server may look into the owner's database for additional information. Secondly, after receiving the retrieved images, the query user may illegally distribute these images to someone unauthorized for benefits. Contribution. This paper protects the privacy.

II. LITERATURE SURVEY

Ref: "Public key encryption with keyword search,**" Author Name:** D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano,

Searchable encryption (SE) schemes enable the query user to search over the encrypted data collections. Most of the existing SE schemes focus on the retrieval of text documents. Some early schemes explore the Boolean search to identify whether or not a query term is present in the encrypted text documents. Afterwards, plenty of methods have been proposed under different threat models to achieve various search functionalities, such as similarity search, multi keyword ranked search, dynamic search, etc. However, few of these schemes are straightforwardly feasible to an image retrieval task. Shashank *et al.*

Ref: "Practical techniques for searches on encrypted data,**"Author Name:** D. X. Song, D. Wagner, and A. Perrig,

Propose a Private Content-based Image Retrieval (PCBIR) scheme which protects the privacy of the query image, but exposing the unencrypted image database to the server directly. Some researchers outsource the computation of image feature extraction to the cloud server in a privacy-preserving manner, which can be the key techniques to the privacy-preserving CBIR outsourcing. Nevertheless, the index construction and similar search on the encrypted features need to be further addressed. In addition, the homomorphic-encryption based schemes usually incur high computation and storage in the area of privacy-preserving CBIR schemes, Lu *etal.* constructed the first privacy-preserving CBIR scheme over the encrypted images. The authors extracted the visual words to represent the images, and then calculated the Jaccard similarity between the two sets of visual words so as toevaluate the similarity between the two corresponding images. The order-preserving encryption and min-hash algorithm are employed to protect the information of the visual words. In another work, Lu *et al.* [23] investigated three image feature protection techniques, i.e. the bitplane randomization, random projection, and randomized unary encoding.

Ref: "Secure indexes.**"**"IACR Cryptology**" Author Name:**E.-J. Goh et al.,

Nevertheless, none of these schemes consider the dishonest query users who may illegally distribute the retrieved images. Actually, it is difficult to design a method to completely prevent illegal distributions. However, it is possible to design certain techniques to deter such illegal behaviors. Watermarking techniques have been widely studied for the copy deterrence in buyer-seller scenarios. For the copy-deterrence purpose, the seller inserts a unique watermark into the image before it being sold to the buyer. If the buyer distributes the copies of the watermarked image, the illegal buyer can be traced by examining the watermark in image. The watermarking techniques can prevent the illegal distributions to some extent. However, there are still several problems that need to be settled to implement watermark based copy deterrence in our scheme.

III. EXISTING SYSTEM

Firstly, a curious cloud server may look into the owner's database for additional information. Secondly, after receiving the retrieved images, the query user may illegally distribute these images to someone unauthorized for benefits.

3.1Disadvantages of Existing System:

The existing searchable encryption schemes usually consider that the query users are fully trustworthy. This is not necessarily true in real-world applications. To the best of our knowledge, this paper is the first work that proposes a searchable encryption scheme, considering the dishonest query users who may distribute the retrieved images to those who are unauthorized.

IV. PROPOSED SYSTEM:

Image owner encrypts original images, index and saves them on cloud server along with user authentication information. Watermark certification authorities (WCA) generate watermarks and send them on cloud server. Cloud server embedded watermarks into encrypted images Image users generate trapdoors and then fire required query. According to query, servers reply with proper results. Hashing algorithm and auditing is used for verification purpose.
If the results are satisfactory to image users, process terminates otherwise alert generation is sent back to image owner.

4.1 Advantage of proposed system:

Zhangs' algorithm was used for encryption, decryption and generating watermark-based images. But now-a-days, watermark-based protocol is used, which improve robustness. If the results are satisfactory to image users, process terminates otherwise alert generation is sent back to image owner.

V. SYSTEM ARCHITECTURE

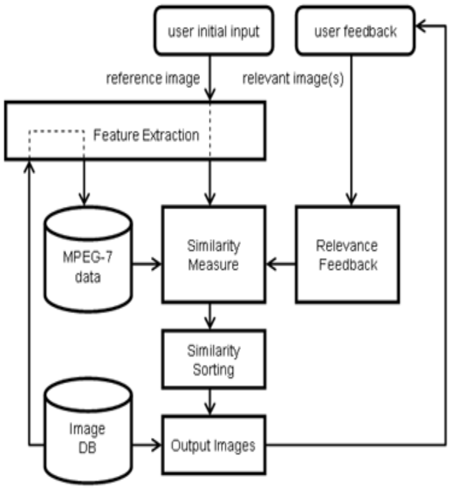

Fig 1: Overall system diagram.

In this paper we presented a privacy preserving and copy deterrence content based image retrieval scheme in a cloud computing scenario.

- The secure AES algorithm is applied toencrypt the visual features.
- Cipher text-only Attack model, the image contentsare secureagainst chosen-plaintext attack model.

V. ALGORITHM USING ADVANCED ENCRYPTION STANDARD (AES)

- In 1997, the U.S. National Institute for Standards and Technology (NIST) put out a public call for a replacement to DES.
- It narrowed down the list of submissions to five finalists, and ultimately chose an algorithm that is now known as the **Advanced Encryption Standard** (**AES**).
- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
- A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack.
- AES is a block cipher that operates on 128-bit blocks. It is designed to be used with keys that are 128, 192, or 256 bits long, yielding ciphers known as AES-128, AES-192, and AES-256.

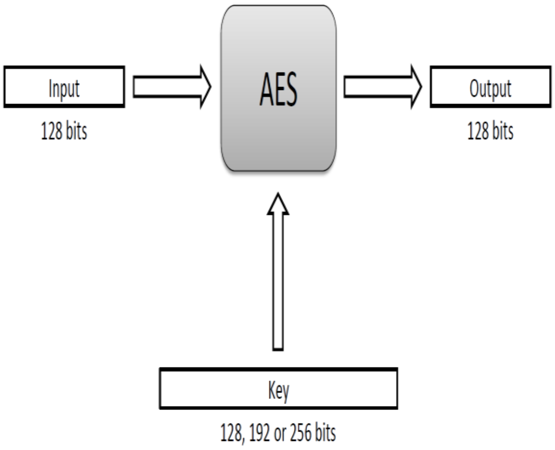

Fig 2: AES bit diagram.

VI. CONCLUSION

As future work, there still are some aspects could be improved. Firstly, the proposed watermarking method cannot be regarded as a very robust one. In this future, we will make more efforts to design watermarking algorithm with better robustness and embedding capacity. We presented a privacy preserving on secure AES and content based image retrieval scheme in cloud computing. The secure AES algorithm is applied to encrypt the visual features.

The similarity scores can be directly calculated with the encrypted features by the cloudserver, which enables the cloud server to rank the images without the additional communication burden. The locality sensitive hashing is utilized to improve the search efficiency. For the first time, we consider the dishonest users in SE schemes and propose a watermark-based protocol to deter the illegal distribution of images. Overall, the image features are secure against Cipher text-only Attack model, the image contents are secure against Chosen-plaintext Attack model, and the search efficiency is improved from $O(n)$ to $O(n')$.

ACKNOWLEDGMENT

I would like to thank Dr.S.Santhosh kumar for his guidance and support for preparing this paper.

REFERENCES

[1] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEETransactions on Parallel and Distributed Systems*, vol. PP, no. 99, p. 2015.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement,"*IEEE*

Transactions on Parallel & Distributed Systems, vol. PP, no.Online, pp. 1–1, 2015.

[3] S. Kamara and C. Papamanthou, “Parallel and dynamic searchable symmetric encryption,” in *Financial Cryptography and Data Security*. Springer, 2013, pp. 258–274.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in *Advances in Cryptology-Eurocrypt*. Springer, 2004, pp. 506–522.

[5] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in *Proc. of IEEE Symposium on Security andPrivacy*. IEEE, 2000, pp. 44–55

[6] E.-J. Goh *et al.*, “Secure indexes.” *IACR Cryptology ePrint Archive*, vol. 2003, p. 216, 2003.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in *Proc. of 13th ACM conference on Computer and communicationssecurity*. ACM, 2006, pp. 79–88.

[8] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, “A novel routing protocol providing good transmission reliability in underwater sensor networks,” *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.

[9] M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient similarity search over encrypted data,” in *Proc. of 28th International Conference on Data Engineering*. IEEE, 2012, pp. 1156–1167.

[10] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, “Achieving usable and privacy-assured similarity search over outsourced cloud data,” in *Proc.of INFOCOM*. IEEE, 2012, pp. 451–459.

[11] Z. Xia, Y. Zhu, X. Sun, and L. Chen, “Secure semantic expansion based search over encrypted cloud data supporting similarity ranking,” *Journalof Cloud Computing*, vol. 3, no. 1, pp. 1–11, 2014.

[12] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multikeyword ranked search over encrypted cloud data,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, 2014.

[13] Z. Fu, X. Sun, Q. Liu, L. ZHOU, and J. SHU, “Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing,” *IEICE Transactions on Communications*, vol. 98, no. 1, pp.190–200, 2015.